Discrete Mathematics

Arthur T. Benjamin, Ph.D.

THE GREAT COURSES®

PUBLISHED BY:

THE GREAT COURSES
Corporate Headquarters
4840 Westfields Boulevard, Suite 500
Chantilly, Virginia 20151-2299
Phone: 1-800-832-2412
Fax: 703-378-3819
www.thegreatcourses.com

Arthur T. Benjamin, Ph.D.

Professor of Mathematics, Harvey Mudd College

Arthur T. Benjamin is a Professor of Mathematics at Harvey Mudd College. He graduated from Carnegie Mellon University in 1983, where he earned a B.S. in Applied Mathematics with university honors. He received his Ph.D. in Mathematical Sciences in 1989 from Johns Hopkins University, where he was supported by a National Science Foundation graduate fellowship and a Rufus P. Isaacs fellowship. Since 1989, Professor Benjamin has been a faculty member of the Mathematics Department at Harvey Mudd College, where he has served as department chair. He has spent sabbatical visits at Caltech, Brandeis University, and the University of New South Wales in Sydney, Australia.

In 1999, Professor Benjamin received the Southern California Section of the Mathematical Association of America (MAA) Award for Distinguished College or University Teaching of Mathematics, and in 2000, he received the MAA Deborah and Franklin Tepper Haimo National Award for Distinguished College or University Teaching of Mathematics. He was named the 2006–2008 George Pólya Lecturer by the MAA.

Professor Benjamin's research interests include combinatorics, game theory, and number theory, with a special fondness for Fibonacci numbers. Many of these ideas appear in his book (coauthored with Jennifer Quinn) *Proofs That Really Count: The Art of Combinatorial Proof*, published by the MAA. In 2006, that book received the MAA's Beckenbach Book Prize. From 2004 to 2008, Professors Benjamin and Quinn served as the coeditors of *Math Horizons* magazine, published by the MAA and enjoyed by more than 20,000 readers, mostly undergraduate math students and their teachers. In 2009, the MAA published Professor Benjamin's latest book, *Biscuits of Number Theory*, coedited with Ezra Brown.

Professor Benjamin is also a professional magician. He has given more than 1000 "mathemagics" shows to audiences all over the world (from primary schools to scientific conferences), where he demonstrates and explains his calculating talents. His techniques are explained in his book *Secrets of Mental Math: The Mathemagician's Guide to Lightning Calculation and Amazing Math Tricks*. Prolific math and science writer Martin Gardner calls it "the clearest, simplest, most entertaining, and best book yet on the art of calculating in your head." An avid game player, Professor Benjamin was winner of the American Backgammon Tour in 1997.

Professor Benjamin has appeared on dozens of television and radio programs, including the *Today* show, CNN, and National Public Radio. He has been featured in *Scientific American*, *Omni*, *Discover*, *People*, *Esquire*, *The New York Times*, the *Los Angeles Times*, and *Reader's Digest*. In 2005, *Reader's Digest* called him "America's Best Math Whiz."

Acknowledgments

It is a pleasure to thank the many people who helped me with *Discrete Mathematics*. First I would like to thank the many students from Harvey Mudd College and other Claremont Colleges who have taken discrete mathematics from me over the last 20 years. I have learned a great deal teaching and working with these highly motivated students. Special thanks are due to Harvey Mudd College students Craig Burkhart, Jennifer Iglesias, Jack Newhouse, Aaron Pribadi, and Elizabeth Reiland; Pitzer College student Scott Garrabrant; and Harvey Mudd College Professor Geoff Kuenning, all of whom offered valuable comments on the first draft of this course. I was very fortunate to be able to present most of these lectures to the students and faculty at Denison University and Roanoke College. I am especially grateful to Professors Sarah Crown, Tom Wexler, Jan Minton, and Roland Minton for their expertise, input, support, and hospitality.

It has been a pleasure working with the ultraprofessional staff of The Teaching Company. Although I know there were many people working on this course behind the scenes, I would especially like to thank Zach Rhoades, Matt Costanza, John Levin, and most of all, Jay Tate.

Last, but not least, I thank my family for their patience and understanding while this course was being created. I must especially thank my wife, Deena Benjamin, who is my light, my inspiration, the love of my life, and my typesetter. This course could not have been made without you!

Arthur T. Benjamin

Table of Contents
Discrete Mathematics

Table of Contents
Discrete Mathematics

Discrete Mathematics

Scope:

Discrete mathematics can be described as an advanced look at the mathematics that we learned as children. In elementary school, we learned to count, did basic arithmetic, and amused ourselves with solving puzzles, ranging from connecting the dots, to coloring, to more sophisticated creative pursuits.

So what exactly is discrete mathematics? Perhaps it is easier to first say what it is not. Most of the mathematics that we are taught in high school—from geometry through calculus—is continuous mathematics. Think of the second hand of a wristwatch or the path traveled by a ball as it is thrown in the air. These objects are typically described by real numbers and continuous functions. By contrast, discrete mathematics is concerned with processes that occur in separate chunks, such as how the seconds or minutes change on a digital watch, or the way the path of the ball would look if we took a few snapshots of its journey. The numbers used in discrete mathematics are whole numbers. Discrete mathematics is the foundation of computer science, where statements are true or false, numbers are represented with finite precision, and every piece of data is stored in a specific place.

In this course, we concentrate on 3 major fields of discrete mathematics: combinatorics, number theory, and graph theory. Combinatorics is the mathematics of counting. How many ways can we rearrange the letters of "Mississippi"? How many different lottery tickets can be printed? How many ways can we be dealt a full house in poker? Central to the answers to these questions is Pascal's triangle, whose numbers contain some amazingly beautiful patterns, which we shall explore.

Number theory, as its name suggests, is the study of the whole numbers: 0, 1, 2, 3, … . Many of their basic properties were taught to us in elementary school without any reason given. We remedy that here and present you with additional surprises. For instance, why can every number be factored into primes in exactly one way? Why do the digits of a multiple of 9 always sum to a multiple of 9? How can we tell if a number is composite, even if we do not know any of its factors? Why are the Fibonacci numbers so beautiful? Although some mathematicians used to boast that number theory would have little practical value beyond arithmetic, its applications are (if you will excuse the pun) numerous, from card shuffling, to ISBNs found in every

book, to Internet security. We will see how number theory forms the basis for public key cryptography, allowing safe and convenient financial transactions over the Internet.

Graph theory allows us to explore relationships between objects in a most effective way. For example, did you know that among any 6 people, there must always be 3 mutual friends or 3 mutual strangers? Graph theory enables us to prove this just by drawing 6 dots on a piece of paper, connected with lines of red for friends and blue for strangers: No matter how the lines are colored, there must exist either an all-red triangle or an all-blue triangle. Graph theory can be used to describe networks that model everything from transportation grids to how computers communicate and store information. We will answer questions like, Using a network of roads, what is the quickest way of getting from one point to another? We will see that this question can be answered using a very efficient algorithm but that a similar-sounding problem (the traveling salesman problem) has no known efficient algorithm.

Throughout this course, we will see some beautiful patterns, leading to some amazing theorems and formulas, but you will not just have to take my word for them. Using nothing more than elementary logic (requiring nothing more sophisticated than a first course in algebra), we will be able to give complete and satisfying explanations to nearly everything presented in the course. In high school, too much of the mathematics is taught as nothing more than a collection of facts or techniques to be mastered without any understanding. In discrete mathematics (and indeed most college-level math courses), the real joy and mastery of the material comes from deep understanding.

Lecture One
What Is Discrete Mathematics?

Scope: We begin with an overview of discrete mathematics. How is it different from the continuous mathematics that is emphasized in high school? With continuous mathematics, you typically deal with infinite sets, such as the set of real numbers or the set of lines in a plane. But discrete mathematics addresses questions that deal with finite sets. With continuous mathematics, you work with real numbers like $\pi = 3.14159\ldots$ and $\sqrt{2} = 1.41421\ldots$, but with discrete mathematics, you work primarily with whole numbers like 0, 1, 2, 3, and so on. In continuous mathematics, you learn to graph functions like lines, parabolas, and circles. But in discrete mathematics, the word "graph" takes on a whole new meaning, where objects are represented by points, and 2 points are connected by a line segment if they are related in some way.

Our course will focus mainly on 3 topics—combinatorics (clever ways of counting), number theory, and graph theory—with applications such as probability, card shuffling, and cryptography. We provide an overview of each of these topics and highlight some of the problems that we will address in this course.

Outline

I. Discrete math is not continuous math.

A. Much of the mathematics we learn in school, most notably calculus, is continuous mathematics, which is the mathematics of how things grow and change continuously.

B. Discrete mathematics is interested in quantities that can be broken into neat little pieces, like pixels on your computer screen, letters or numbers in your password, or directions on how to drive from one place to another.

C. Some typical problems in discrete math are inspired by a deck of cards.

1. How many ways can 52 cards be arranged?

2. How many 5-card poker hands exist?

3. How many 5-card hands have at least 1 ace?

D. Continuous mathematics is like an old-fashioned analog clock whose second hand moves continuously, but discrete math is like a digital watch that changes 1 second at a time.

E. Discrete mathematics is the foundation of computer science, which works with 0s and 1s, and logical statements that are true or false.

F. Just as the world has changed from analog to mainly digital in most of its technology, it is time for students to learn mathematics that is both continuous and discrete.

G. Our course will focus on 3 major topics, combinatorics (Lectures Two through Eight), number theory (Lectures Nine through Fifteen), and graph theory (Lectures Sixteen through Twenty-Three).

II. What is combinatorics?

A. Combinatorics is the mathematics of counting things.

B. For example, the number of binary code words of length n is 2^n.

C. When $n = 1, 2, 3, 4, \ldots$, the number of code words of length n with no consecutive 0s is 2, 3, 5, 8, … . These are the Fibonacci numbers!

III. What is number theory?

A. Number theory is the study of whole numbers (0, 1, 2, 3, 4, …) for their intrinsic beauty.

B. We will learn beautiful facts about numbers, but we will also learn the reasons behind them.

1. For example, why do the digits of a multiple of 9 sum to a multiple of 9?

2. We will learn how to see at a glance that a number like 2354 is a multiple of 11, using something called modular arithmetic, and we will apply it to ISBNs that appear on every book.

3. We will learn how numbers can be expressed uniquely as the sum of powers of 2, as well as the product of prime numbers.

4. We will also apply number theory to card shuffling, error-detecting codes, and public key cryptography.

IV. What is graph theory?

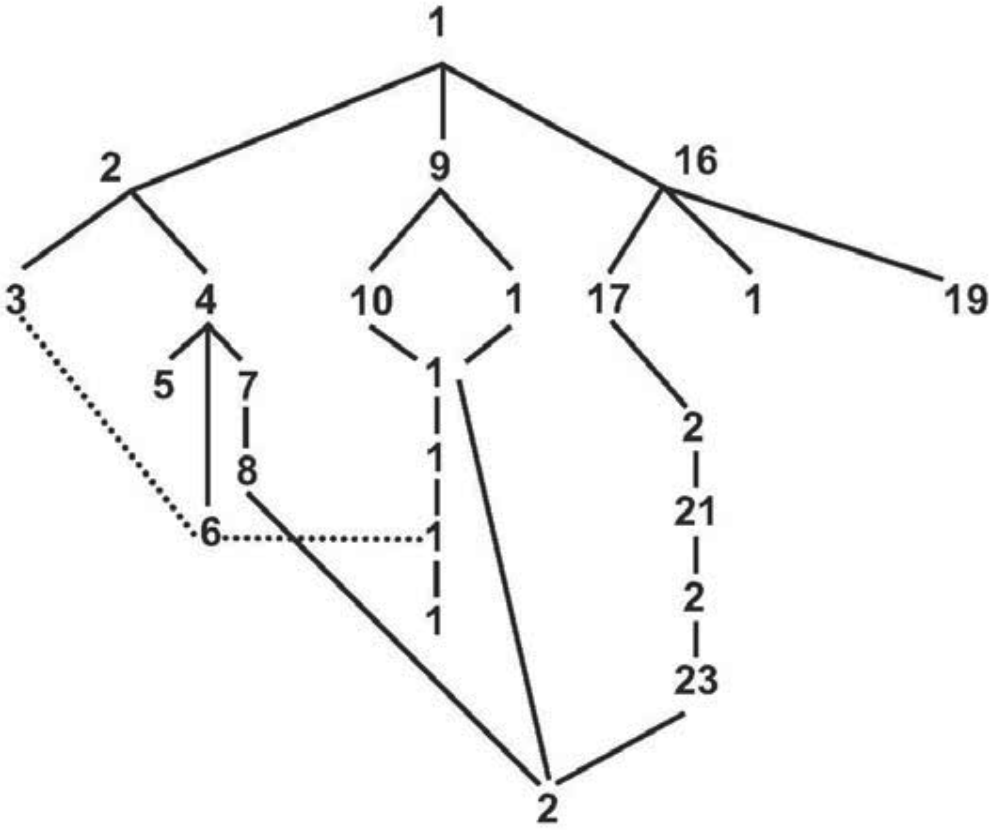
A. We illustrate a typical graph, known as the subset graph.

1. The set $S = \{1, 2, 3\}$ has 8 subsets: $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1, 2, 3\}$, and the empty set $\{\ \}$.

2. Each vertex in our graph represents a subset, and 2 subsets are connected by an edge if their sizes differ by 1 and the smaller set is a subset of the larger set.
3. When you draw this graph, you will see a cube. Likewise, when you draw the subset graphs of the set { }, {1}, {1, 2}, you see a point, a line, and a square, respectively. The subset graph of {1, 2, 3, 4} will look like a 4-dimensional cube.

B. Graph theory can prove that among any 6 people, there must be at least 3 mutual friends or 3 mutual strangers.

C. Even this course in discrete mathematics can be modeled with a graph. We present here a graph where Lecture *A* points to Lecture *B* if *A* is a prerequisite to *B*. Dotted lines indicate lectures that have some topics in common.



D. Graph theory can also be used to represent transportation problems.

V. Our approach to discrete mathematics: Discrete math can be thought of as sophisticated math for kindergartners. After all, we will do counting, arithmetic, connecting the dots, and coloring.

A. Discrete math has applications that are both serious and recreational.

B. Its only prerequisite is high school algebra.

C. It can be described in 2 words: relevant and elegant!

Suggested Reading:

Gross and Harris, *The Magic of Numbers*.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*.

Rosen, *Discrete Mathematics and Its Applications*.

Scheinerman, *Mathematics: A Discrete Introduction*.

Questions to Consider:

1. Which of these quantities are more likely to be described as discrete instead of continuous?

a. The number of ways to fill out a lottery ticket.

b. The area of a geometric figure.

c. The annual rainfall of a particular town.

d. The pages of a book.

e. The number of cars that pass by your home today.

f. The average speed of the cars that pass by your home today.

g. The length of time of a baseball game.

h. The final score of a baseball game.

2. A ternary code word has digits that can be 0, 1, or 2. For example, there are 9 ternary code words of length 2: 00, 01, 02, 10, 11, 12, 20, 21, and 22.

a. How many ternary code words have length 3?

b. How many ternary code words have length n?

3. Explain why the decimal expansion of a fraction m/n (where m and n are positive integers) must either terminate or have a repeated part, where the length of the repeated part is at most $n - 1$. For example, the fraction $3/7 = 0.428571428571\ldots$ has a repeated part of length 6.

4. Which fractions $1/n$ have a terminating decimal expansion? The first few examples are $1/2 = 0.5$, $1/4 = 0.25$, $1/5 = 0.2$, $1/8 = 0.125$, and $1/10 = 0.1$.

5. Consider the positive divisors of 72: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, and 72. Draw a graph where each divisor is represented by a vertex, and 2 vertices are connected by an edge if one of them is exactly 2 or 3 times as large as the other. Find the other number whose graph will have the same shape as this one.

Lecture Two
Basic Concepts of Combinatorics

Scope: Most counting questions ultimately boil down to 2 rules: the rule of sum and the rule of product. Using these rules, we address the question "From a collection of n distinct objects, how many ways can you select k of them?" under various assumptions. If the order of the objects is important and repetition is allowed, we call this a sequence, and there are n^k ways. If repetition is not allowed, then this is called an arrangement, and there are $n!/(n-k)!$ ways. When $k = n$, this says that all n objects can be arranged in $n!$ ways. If order does not matter and repetition is not allowed, this situation is called a subset or a combination, and the number of combinations is given by $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, which is one of the most important numbers in combinatorics. Once we understand these basic concepts, we can determine the probability of being dealt any hand in poker, from the highest-ranking hand (a royal flush) down to the lowliest garbage hands, containing no pairs, straights, or flushes.

Outline

I. We begin by asking a simple question—"How many?"—that has at least 4 interpretations.

A. Any discrete math course will contain a significant portion devoted to combinatorics, the mathematics of counting.

B. How many ways can we pick 5 numbers from 1 to 10? There are 4 ways to answer this depending on 2 factors.

1. Does order matter?

2. Can you repeat numbers?

C. If order matters and repetition is allowed, we call that a sequence. Zip codes are sequences: 31415 is not equal to 31451.

D. If order matters and repetition is not allowed, this is called an arrangement. In a horse race, the order of the first 3 horses to finish may matter to you.

E. If repetition is not allowed, but order does not matter, this is called a subset or combination. For example, a typical poker hand consists of 5 cards, where the order of the cards does not matter.

F. The fourth situation, where order does not matter and repetition is allowed, will be discussed later.

II. Rule of sum and product.

A. The rule of sum states that if an action is performed by making A choices or B other choices, then it can be performed $A + B$ ways.

1. For example, if I can choose from 4 short-sleeved shirts and 6 long-sleeved shirts, then I have 10 choices of shirts.

2. The rule of sum can also be described in terms of sets; we will do so in a future lecture.

B. The rule of product states that if an action can be performed by making A choices followed by B choices, then it can be performed AB ways.

1. For example, if I have 10 shirts and 8 pants, then I have 80 different outfits.

2. If a label consists of a letter (A, B, or C) followed by a number (from 1 to 5), then there are $3 \times 5 = 15$ labels.

3. Each card in a deck has 1 of 13 values (from ace to king) and a choice of 4 suits, so there are $13 \times 4 = 52$ cards in a deck.

4. In general, $n!$ (pronounced "n factorial") is the number of ways to arrange n objects. This is also known as a permutation.

III. Another extremely important number in combinatorics is the binomial coefficient.

A. The binomial coefficient is denoted by $\binom{n}{k}$, pronounced "n choose k." Another common notation is $C(n, k)$ (where the C stands for "choices" or "combination").

B. There are several equivalent ways to define $\binom{n}{k}$.

1. It is the number of ways to choose k objects from n, where order is not important and repetition is not allowed. For example, there are $\binom{52}{5}$ ways to create a 5-card poker hand.

2. Officially, $\binom{n}{k}$ is the number of size-k subsets of the set $\{1, 2, \ldots, n\}$. For example, $\binom{4}{2} = 6$ counts $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, and $\{3, 4\}$.

C. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. For example, $\binom{10}{3} = 10!/3!7! = 10 \times 9 \times 8/3! = 720/6 = 120$.

D. Notice $\binom{n}{0} = 1$, which makes sense since there is 1 way to pick 0 objects out of n (or 1 size-0 subset of $\{1, \ldots, n\}$).

IV. Poker hands are a natural application for the binomial coefficient.

A. The number of 5-card poker hands is $\binom{52}{5} = 2{,}598{,}960$.

B. How many are full houses (3 of one value and 2 of another)? There are 13 choices for which card value is tripled, then 12 choices for which card value is doubled, then $\binom{4}{3}$ ways to assign suits to the tripled value, then $\binom{4}{2}$ ways to assign suits to the doubled value. Multiplying these, we get $13 \times 12 \times 4 \times 6 = 3744$.

C. How many hands have exactly 1 pair? There are 13 choices for the paired value, then $\binom{4}{2} = 6$ ways to decide which 2 of the 4 possible cards will make up the pair, then $\binom{12}{3} = 220$ ways to pick the 3 other values. Then we assign suits for those cards, in $4^3 = 64$ ways. Multiplying gives us 1,098,240 ways to be dealt 1 pair, and the probability is about 0.42.

V. Summary: How many ways are there to select k objects from n distinct objects? Provide numerical answers when $n = 10$ and $k = 5$.

A. Sequences: If order matters and repetition is allowed: n^k ways, equal to 100,000.

B. Arrangements: If order matters but repetition is not allowed: $n!/(n-k)!$, equal to 30,240.

C. Subsets: If order does not matter and repetition is not allowed: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, equal to 252.

D. Multisubsets: If order does not matter and repetition is allowed. The answer is 2002, but we will save the formula for a future lecture.

When $n = 10$, $k = 5$	Order matters	Order does not matter
Repetition allowed	sequences $n^k = 100{,}000$	multisubsets [formula given in Lecture Five] = 2002
Repetition not allowed	arrangements $n!/(n-k)! = 30{,}240$	subsets $\frac{n!}{k!(n-k)!} = 252$

Suggested Reading:

Gross and Harris, *The Magic of Numbers*, chap. 2.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 1.

Rosen, *Discrete Mathematics and Its Applications*, chap. 4.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 7–8.

Tucker, *Applied Combinatorics*, chap. 5.

Questions to Consider:

1. Which of the following counting situations are best described as subsets, instead of arrangements?

a. The number of lottery tickets that contain 4 or more of the winning numbers.

b. The number of ways to choose which 9 students get to play on the baseball team.

c. The number of ways to assign 9 students positions to play on a baseball team.

d. The number of coin flip sequences of length 5 (for example, HHTTH).

e. The number of coin flip sequences of length 5 that have exactly 3 heads.

2. Suppose that 5 distinct 6-sided dice are rolled (colored red, yellow, green, blue, and purple).

a. How many different outcomes are possible?

b. How many outcomes with 5 consecutive numbers are possible?

c. How many full houses, with 3 dice showing one value and 2 dice showing another, are possible?

d. How many outcomes where the total is even are possible?

Lecture Three
The 12-Fold Way of Combinatorics

Scope: The 12-fold way gives a nice road map of what we are doing in combinatorics: It is a combinatorics problem about combinatorics problems. Do not worry about needing to understand everything in this lecture before continuing with later lectures; instead, return to this lecture after you have gained more combinatorial experience from later lectures. We consider 12 different versions of the question "How many ways can we place x pieces of candy into b bags?" The answer depends on whether the objects are distinguishable or identical, whether the bags are distinguishable or identical, and whether the bags can hold any number of objects, can hold at most 1 object, or must have at least 1 object.

Outline

I. The 12-fold way of combinatorics is a question with 12 interpretations.

A. Consider this question: How many ways can x pieces of candy be distributed among b bags?

B. The answer will depend on 3 factors: Are the candies distinguishable? Are the bags distinguishable? Can the bags have any number of candies, can they have at most 1 candy, or must they have at least 1 candy?

C. Hence there are $2 \times 2 \times 3 = 12$ interpretations of this question.

D. The answers will be entered into a table, called the 12-fold way table.

Candies (x)	Bags (b)	Unrestricted	≤ 1	≥ 1
D	D	(D, D, U)	(D, D, <)	(D, D, >)
I	D	(I, D, U)	(I, D, <)	(I, D, >)
D	I	(D, I, U)	(D, I, <)	(D, I, >)
I	I	(I, I, U)	(I, I, <)	(I, I, >)

E. Notice that if $x > b$, then there are 0 ways to distribute candy into bags so that each bag gets at most 1 candy. When $b > x$, there are 0 allocations where each bag gets at least 1 candy. Thus, we will focus on those situations where the answer is not 0.

F. We will denote our 12 situations using the ordered triple (candy, bags, capacity), where an entry of D denotes distinguishable; I denotes identical (or indistinguishable); and the third entry is U (for unrestricted), < (for at most 1 candy per bag), or > (for at least 1 candy per bag). For example, (D, I, >) denotes the situation where the candies are distinguishable, the bags are identical, and each bag requires at least 1 candy. For such situations, we will assume that x is at least as large as b.

II. Five of the table entries can be entered using what we know already from Lecture Two.

A. Situation (D, D, U) can be performed b^x ways, since each of the x candies can be placed in any of the b bags.

B. Situation (D, D, <) can be performed $b(b-1)(b-2)\cdots(b-x+1)$ ways, since the first candy has b choices, the second candy has $b-1$ choices, … , and the x^{th} candy has $(b-x+1)$ choices. This answer can be written more compactly as $b!/(b-x)!$

C. For the situation (I, D, <), the candies are identical, and each bag can contain at most 1 candy, so all we have to decide is which of the b bags receive a candy and which ones do not. This can be done $\binom{b}{x}$ ways (the binomial coefficient "b choose x").

D. Finishing the second column, the entries (D, I, <) and (I, I, <) are 0 when x is greater than b, and otherwise are 1, since each candy is simply put in its own bag (and all bags look alike).

III. Candies and bars: 2 other entries of our table will have answers that are given by binomial coefficients.

A. The situation (I, D, U) can be performed $\binom{x+b-1}{x}$ ways.

1. This can be seen by representing each allocation with x candies (represented by circles) and $b-1$ bars (which act as dividers between bags).

2. For example, the allocation OO|OOOOO|O|O|O represents the situation where bags 1, 2, 3, 4, and 5 get 2, 5, 1, 1, and 1 candy, respectively.

3. The allocation |OOO|O||OOOOOO represents bags 1, 2, 3, 4, and 5 getting 0, 3, 1, 0, and 6 candies, respectively.

4. Altogether, the number of ways to arrange 10 candies and 4 bars (14 objects total) is $\binom{14}{10}$.

B. The situation (I, D, >) can be performed $\binom{x-1}{b-1}$ ways.

1. To see this, just put at least 1 candy into each bag, and solve the previous (unrestricted) problem.

2. Replacing x with $x - b$ gives us $\binom{(x-b)+b-1}{x-b}$, which equals $\binom{x-1}{x-b}$, which equals $\binom{x-1}{b-1}$.

IV. Stirling numbers answer the question when the candies are distinguishable, the bags are identical, and each bag gets at least 1 candy.

A. Here we analyze the situations (D, I, >), (D, D, >), and (D, I, U).

B. We define the answer to (D, I, >) to be $S(x, b)$, known as a Stirling number (of the second kind). For example, there are $S(11, 4)$ ways to distribute 11 distinct candies into 4 identical-looking bags, where each bag must get at least 1 candy. We will derive a formula for $S(x, b)$ when we study the principle of inclusion-exclusion in Lecture Six.

C. We can also compute $S(x, b)$ recursively, by considering whether or not candy number x is in its own bag. For example, $S(11, 4) = S(10, 3) + 4S(10, 4)$, since the first term counts those allocations where the 11^{th} candy is in its own bag, and the second term counts those allocations where the 11^{th} candy is not alone.

D. The answer to the situation (D, D, >) is $b!S(x, b)$, since once we fill each identical bag, we can label the bags $b!$ ways to make them distinguishable.

E. The situation (D, I, U) counts the ways to allocate the candies into any number of nonempty bags (from 1 to b), so the answer is $S(x, 1) + S(x, 2) + \cdots + S(x, b)$, or using summation notation, $\sum_{k=1}^{b} S(x,k)$.

F. When $x = b = n$, this sum is sometimes denoted as $B(n)$, the n^{th} Bell number, which counts the number of ways to partition a set into any number of parts.

V. Integer partitions.

A. The situation (I, I, >) is called the integer partitioning problem, since it counts the ways that the integer x can be expressed as the sum of b positive numbers, where order is not important.

B. There is no closed formula for this problem, so we define the answer to be $p_b(x)$.

C. For example, $p_3(6) = 3$, since $6 = 4 + 1 + 1$ or $3 + 2 + 1$ or $2 + 2 + 2$.

D. The smallest bag either contains 1 candy or it does not. The number of allocations where the smallest bag has exactly 1 candy is $p_{k-1}(n - 1)$. The number where the smallest bag (and therefore all bags) have more than 1 candy is $p_k(n - k)$, since we place 1 candy in each bag, which reduces it to a smaller problem where each bag will receive at least 1 more candy.

E. Thus, $p_k(n) = p_{k-1}(n - 1) + p_k(n - k)$.

F. Finally, the situation (I, I, U) counts allocations into any number of bags (b or fewer) and therefore has $\sum_{k=1}^{b} p_k(b)$ allocations.

G. When $x = b = n$, this is denoted by $p(n)$, the number of partitions of n (into any number of parts).

VI. Summary of results: This completes our 12-fold way table, as displayed here.

Candies (x)	Bags (b)	Unrestricted	≤ 1	≥ 1
D	D	b^x	$b!/(b-x)!$	$b!S(x, b)$
I	D	$\binom{x+b-1}{x}$	$\binom{b}{x}$	$\binom{x-1}{b-1}$
D	I	$\sum_{k=1}^{b} S(x,k)$	1 if $x \le b$ 0 if $x > b$	$S(x, b)$
I	I	$\sum_{k=1}^{b} p_k(x)$	1 if $x \le b$ 0 if $x > b$	$p_b(x)$

A. Here are its entries when $x = 5$ and $b = 10$.

Candies ($x = 5$)	Bags ($b = 10$)	Unrestricted	≤ 1	≥ 1
D	D	100,000	30,240	0
I	D	2002	252	0
D	I	52	1	0
I	I	7	1	0

B. Here are its entries when $x = 10$ and $b = 5$.

Candies ($x = 10$)	Bags ($b = 5$)	Unrestricted	≤ 1	≥ 1
D	D	9,750,625	0	5,103,000
I	D	1001	0	126
D	I	86,462	0	42,525
I	I	30	0	7

Suggested Reading:

Bogart, *Introductory Combinatorics*, chap. 2.

Graham, Knuth, and Patashnik, *Concrete Mathematics*.

Stanley, *Enumerative Combinatorics*, chap. 1.

Questions to Consider:

1. Find the category of objects and containers that best describes each of these problems. For example, putting individual samples of DNA into lab bottles would be an instance of distributing distinct objects to identical containers, where each container could hold at most 1 object—which we write as (D, I, ≤ 1).

a. Distributing identical candies to children so that each child gets at least 1 candy.

b. Distributing distinct candies to children that allows for some children to get no candies.

c. Deciding who does which chores among a group of housemates.

d. Same as (c) above, but nobody does more than 1 chore.

e. Awarding $100 cash prizes to the best costumes at a party.

f. Deciding on first, second, and third prize at a music competition.

g. Breaking a class of students into 5 study groups.

h. Creating 5 or fewer study groups from a group of students.

2. Determine the number of ways that 10 distinct pieces of candy can be placed into k identical bags when $k = 1$, $k = 2$, $k = 9$, and $k = 10$, with each bag getting at least 1 piece. In other words, find a formula for the Stirling numbers: $S(10, 1)$, $S(10, 2)$, $S(10, 9)$, and $S(10, 10)$. More generally, find $S(n, 1)$, $S(n, 2)$, $S(n, n - 1)$, and $S(n, n)$.

3. Same problem as above, but now the 10 candies are identical. In other words, find the partition numbers $p_1(10)$, $p_2(10)$, $p_9(10)$, and $p_{10}(10)$. More generally, find $p_1(n)$, $p_2(n)$, $p_{n-1}(n)$, and $p_n(n)$.

4. Find a numerical answer for $S(6, 4)$, the number of ways 6 distinct candies can be placed into 4 identical-looking, nonempty bags.

5. Find a numerical answer for $p_4(6)$, the number of ways 6 identical candies can be placed into 4 identical-looking, nonempty bags.

Lecture Four
Pascal's Triangle and the Binomial Theorem

Scope: Mathematics is the science of patterns. Perhaps nothing in mathematics contains more beautiful patterns than Pascal's triangle. The entries of Pascal's triangle are simply the binomial coefficients. Specifically, the k^{th} entry of row n is the counting number $\binom{n}{k}$. Consequently, each row begins and ends with the number 1, and the other numbers are the sums of the 2 numbers above them in the previous row. When we interpret $\binom{n}{k}$ as the number of ways that a size-k committee can be created from a group of n people, we can explain many of the triangle's patterns. We also explore the binomial theorem, which allows many patterns in Pascal's triangle to be proved by algebraic method.

Outline

I. The French mathematician Blaise Pascal discovered Pascal's triangle in 1654 when analyzing a problem that arose from gambling, called the problem of points.

A. The problem of points considers 2 players, A and B, playing a game of chance. Each game is worth 1 point, and whoever reaches n points first will win a prize worth d dollars. Each game is equally likely to be won by A or B. Currently player A has a points and player B has b points. If the players decide to stop playing the match at this point, then what is the fair way to split the money?

B. Pascal's triangle was actually known to mathematicians in China and India at least 500 years earlier, but Pascal was the first mathematician to systematically explore its many properties in his treatise *Traité du Triangle Arithmétique*, written in 1655.

C. The first 7 rows of Pascal's triangle are as follows:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1.

1. Notice that each row begins and ends with 1. In between, the numbers are the sum of the 2 entries above them.

2. The second column contains the integers 1, 2, 3, … .

3. The third column contains the triangular numbers 1, 3, 6, 10, … . The sums of consecutive numbers in this column are the perfect squares.

4. The fourth column contains the tetrahedral numbers.

D. Here is the official definition of Pascal's triangle. For $n \geq 0$, the elements of row n are the binomial coefficients:

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots \binom{n}{n}.$$

E. For example, row 4 (the fifth row) looks like

$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$, numerically equal to 1 4 6 4 1.

II. Pascal's triangle: patterns and proofs.

A. Using the definition of Pascal's triangle, we can find lots of patterns, which we shall prove.

B. Pascal's triangle is symmetric: $\binom{n}{k} = \binom{n}{n-k}$.

1. This can be proved using factorials:

$$\binom{n}{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

2. This can also be proved combinatorially by noting that the number of ways to choose k objects out of n is the same as the number of ways to *not* choose $n - k$ elements out of n.

C. Each row begins and ends with $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$.

D. For $0 < k < n$, we have $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

1. This can be proved algebraically using factorials.

2. But it is much cleaner to prove it combinatorially by noting that $\binom{n}{k}$ is the number of size-k committees from a class of n students. The number of committees that do not use student n is $\binom{n-1}{k}$. The number that do use student n is $\binom{n-1}{k-1}$.

E. In general, we have

$$\binom{5}{0}+\binom{5}{1}+\binom{5}{2}+\binom{5}{3}+\binom{5}{4}+\binom{5}{5} = 2^5$$

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n} = 2^n$$

1. This can be expressed more compactly using sigma notation: $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.

2. This is proved combinatorially as follows: We ask the question, "From a class of n students, how many ways are there to create a committee?" On the one hand, since a committee can have any size from 0 to n, we get the sum. On the other hand, to create a committee, we can decide, student by student, if they are in or out of the committee, which can be done 2^n ways.

III. The binomial theorem connects Pascal's triangle with algebra.

A. Observe that $(x + y)^2 = x^2 + 2xy + y^2$, and $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$, whose coefficients 1 2 1 and 1 3 3 1 come from Pascal's triangle.

B. The binomial theorem says that this is no accident. For $n \geq 0$, we have $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

1. Here is a combinatorial proof. How many ways are there to distribute n distinct pieces of candy to x girls and y boys?

2. On the one hand, this can be done $(x+y)^n$ ways.

3. On the other hand, for $0 \leq k \leq n$, there are $\binom{n}{k} x^k y^{n-k}$ ways to allocate the candies so that the girls get exactly k of the n candies. Summing over all k gives the right side of the identity.

C. Notice that when we set $x = y = 1$, the binomial theorem gives us $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

D. When $x = -1$ and $y = 1$, we get the skip sum identity: $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$.

IV. More properties and probabilities.

A. The hockey stick identity says that:

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}.$$

B. Another intriguing property is that the number of odd numbers in the n^{th} row of Pascal's triangle is 2^b, where b is the number of 1s in the binary expansion of n.

C. Binomial probabilities. If a fair coin is flipped 10 times, the probability of getting exactly 3 heads is $\binom{10}{3}/2^{10}$, since among the 2^{10} equally likely sequences, there are $\binom{10}{3}$ ways to select for which 3 of them are heads.

D. If the coin is biased so that each flip has heads probability 0.4, then the probability of exactly 3 heads is $\binom{10}{3}(0.4)^3(0.6)^7$.

V. The problem of points is a problem of binomial probabilities.

A. A and B are flipping a fair coin. Each time the coin lands heads, A wins a point; each time the coin lands tails, B wins a point. Whoever first reaches a score of 10 points wins $100. Currently A has 9 points and B has 8 points, and they decide to stop playing. What is the fair way to split the $100?

B. The answer is that A should get $75 and B should get $25. Pascal gave 3 reasons.

C. One way to see this is by considering the next flip and reducing it to a smaller problem. If A wins the next flip (with probability ½), then the score is 10-8 and A would win $100. If B wins the next flip (with probability ½), then the score is 9-9, and the fair settlement would be that A should get $50. Taking the average of these 2 equally likely results, A deserves $75.

D. By a similar calculation, we can show that the probability that A wins from the score 9-8 is ¾, and the probability that B wins is ¼. So A should receive a payout that is 3 times as much as B. For a 3:1 payout ratio, A deserves $75 and B deserves $25.

E. The third strategy is to notice that from the score 9-8, the match can last at most 2 more games. Let us insist that they play 2 games (even if A wins the first game). This yields 4 possible equally likely outcomes: AA, AB, BA, and BB (listing the winners of games 1 and 2). Since A wins the match in 3 of these 4 scenarios, A deserves a 3:1 payout ratio as before.

F. This last approach works for other scores. Suppose the score is 7-6, so that A needs to win 3 games and B needs to win 4 games. The match can last at most 6 more games, so let us insist that they play all 6 games.

1. There are $2^6 = 64$ equally likely outcomes.

2. A wins the match if he can win 3 or 4 or 5 or 6 of these games. The number of ways this can happen is

$$\binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6} = 20 + 15 + 6 + 1 = 42 \text{ ways.}$$

3. B wins the match if A wins 0, 1, or 2 of these 6 games. The number of ways this can happen is $\binom{6}{0} + \binom{6}{1} + \binom{6}{2} = 1 + 6 + 15 = 22$.
4. Hence A and B should be paid in a 42:22 ratio. That is, A deserves \$100(42/64) = \$65.625, and B deserves \$100(22/64) = \$34.375.

Suggested Reading:

Edwards, *Pascal's Arithmetical Triangle*.

Gross and Harris, *The Magic of Numbers*, chap. 6.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 3.

Rosen, *Discrete Mathematics and Its Applications*, chap. 4.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 16.

Questions to Consider:

1. What is row 8 of Pascal's triangle? Based on that, determine the value of $\binom{8}{3}$.
2. Use the binomial theorem to show that $\sum_{k=0}^{n}\binom{n}{k}2^k = 3^n$.
3. Give a combinatorial proof that $\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\binom{n}{6}+\cdots = 2^{n-1}$ by answering the question "If a deck of n cards is dropped, how many ways can an even number of cards be face up?"
4. Combinatorially prove the hockey stick identity:
$\binom{3}{3}+\binom{4}{3}+\binom{5}{3}+\binom{6}{3}+\binom{7}{3}+\binom{8}{3}+\binom{9}{3}=\binom{10}{4}$.
(Hint: Begin with the question "How many ways are there to choose 4 hockey players from 10 players, where the players are wearing jerseys numbered 1 through 10?")
5. Solve the problem of points when the score is 6-5 in a match to 10 points, with the winner receiving \$100. That is, if the match were to end right now, what would be the fair way to split the \$100 prize?

Lecture Five

Advanced Combinatorics—Multichoosing

Scope: How many ways can we choose 3 scoops of ice cream from 31 flavors, assuming that flavors are allowed to be repeated? If the order matters (as they would if they were placed on a cone), then there are $31^3 = 29{,}791$ possibilities. But if the order of the flavors does not matter (like when they are placed in a cup), then the problem is trickier. Using the method of "stars and bars," we show that there are $\binom{33}{3} = 5456$ possibilities. Indeed, the same technique can be shown to answer several related questions, such as "How many ways can we distribute k identical pieces of candy to n hungry children?" We also consider the same question when the candies are distinguishable and we are told how many candies each child is allowed to receive. This leads to the notion of multinomial coefficients and the multinomial theorem, where objects can be assigned more than 2 outcomes.

Outline

I. We warm up with ice cream.

A. A restaurant has 31 flavors of ice cream. How many triple cones are possible? (On a cone, order is important.)

B. If flavors can be repeated, there are $31^3 = 29{,}791$ possibilities.

C. If flavors cannot be repeated, there are $31 \times 30 \times 29 = 26{,}970$ possibilities.

D. How many triple cups are possible? (In a cup, order is not important.)

E. If flavors cannot be repeated, then there are simply $\binom{31}{3} = (31 \times 30 \times 29)/3! = 4495$ cups.

F. If flavors can be repeated, the answer is not $31^3/3!$.

G. We can answer this by breaking the sum into 3 cases, depending on whether it had 1, 2, or 3 flavors represented for a total of $\binom{31}{3} + 2\binom{31}{2} + \binom{31}{1} = 5456$ ways. But this approach will not easily work when the number of scoops is large.

II. Multichoosing is the counting problem when order does not matter and repetition is allowed (mentioned in Lecture Two).

A. We define the number $\left(\!\binom{n}{k}\!\right)$ to be the number of ways to choose k objects from a set of n objects where order is not important and repetition is allowed. This is pronounced "n multichoose k."

B. For example, $\left(\!\binom{31}{3}\!\right) = 5456$.

C. $\left(\!\binom{3}{2}\!\right) = 6$ counts 11, 12, 13, 22, 23, and 33.

D. $\left(\!\binom{2}{3}\!\right) = 4$ counts 111, 112, 122, and 222.

E. We prove that $\left(\!\binom{3}{10}\!\right) = \binom{12}{10}$ using the method of stars and bars.

1. $\left(\!\binom{3}{10}\!\right)$ counts 10 scoops in a big cup, from a set of 3 possible flavors.

2. The allocation ****|**|**** means 4 scoops of flavor 1, 2 scoops of flavor 2, and 4 scoops of flavor 3. This corresponds to the multisubset {1, 1, 1, 1, 2, 2, 3, 3, 3, 3}.

3. The allocation **|********| would signify 2 scoops of flavor 1, 8 scoops of flavor 2, and 0 scoops of flavor 3. This corresponds to the multisubset {1, 1, 2, 2, 2, 2, 2, 2, 2, 2}.

4. The allocation ****||****** signifies 4 scoops of flavor 1, 0 scoops of flavor 2, and 6 scoops of flavor 3.

5. Each allocation can be represented by arranging 10 stars and 2 bars, which can be done $\binom{12}{2} = \binom{12}{10}$ ways.

Thus $\left(\!\binom{3}{10}\!\right) = \binom{12}{10}$.

F. In general, $\left(\!\binom{n}{k}\!\right)$ is the number of ways to arrange k stars and $n - 1$ bars. Therefore, we have the multichoose formula $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$.

G. For example, $\left(\!\binom{31}{3}\!\right) = \binom{33}{3} = 5456$.

III. Applications and identities.

A. How many ways are there to distribute k identical candies to n hungry ninjas?

B. This can also be represented by stars and bars. For example, ****|**|**** means that ninja 1 gets 4 candies, ninja 2 gets 2 candies, and ninja 3 gets 4 candies. This corresponds to the multisubset {1, 1, 1, 1, 2, 2, 3, 3, 3, 3}.

C. Thus, the number of allocations is $\binom{12}{2} = \binom{12}{10}$ ways.

D. In general, n ninjas can share k identical candies in $\left(\!\binom{n}{k}\!\right)$ ways.

E. Now suppose each ninja must get at least 1 candy. After giving each ninja 1 candy, the problem reduces to distributing $k - n$ candies to n ninjas. This can be done $\left(\!\binom{n}{k-n}\!\right)$ ways, which simplifies to $\binom{k-1}{n-1}$.

F. In backgammon, the number of ways to distribute 15 identical checkers among 6 distinct points is $\left(\!\!\binom{6}{15}\!\!\right)$.

G. To get the number of positions that use 15 checkers or fewer, you could write the answer as $\left(\!\!\binom{6}{15}\!\!\right) + \left(\!\!\binom{6}{14}\!\!\right) + \cdots + \left(\!\!\binom{6}{0}\!\!\right)$. But this answer simplifies to $\left(\!\!\binom{7}{15}\!\!\right)$, since we can think of this as distributing 15 identical checkers among 7 points, where the 7th point contains all the "missing" pieces.

H. This argument generalizes to show $\sum_{k=0}^{m}\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+1}{m+1}$.

IV. We can generalize from binomial coefficients to multinomial coefficients.

A. How many ways can we distribute 11 distinct candies so that Mara gets 1, Patty gets 2, Ira gets 4, and Stephen gets 4?

B. This is equivalent to the numbers of ways to arrange the letters in the word "Mississippi."

C. The number of ways this can be done, by choosing the position of the M, then the 2 positions for the Ps, then 4 positions for the Is is $\binom{11}{1}\binom{10}{2}\binom{8}{4}$, which simplifies to 11!/(1!2!4!4!), denoted $\binom{11}{1,2,4,4}$, and is called a multinomial coefficient.

D. Binomial coefficients are a special case: $\binom{n}{k} = \binom{n}{k,\, n-k}$.

E. The binomial theorem generalizes to multinomial coefficients, called the multinomial theorem:

$(x+y+z)^n = \sum\binom{n}{a,b,c}x^a y^b z^c$, where the numbers a, b, and c can be any nonnegative numbers that sum to n.

F. The general version says that

$$(x + y + \cdots + z)^n = \sum \binom{n}{a, b, \ldots, c} x^a y^b \cdots z^c ,$$

where the numbers a, b, … , c can be any nonnegative numbers that sum to n.

Suggested Reading:

Gross and Harris, *The Magic of Numbers*, chaps. 4, 7.

Rosen, *Discrete Mathematics and Its Applications*, chap. 4.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 16–17.

Tucker, *Applied Combinatorics*, chap. 5.

Questions to Consider:

1. Find the number of solutions to the equation $w + x + y + z = 100$, where w, x, y, and z are required to be nonnegative integers.

2. How does your answer change if w, x, y, and z are required to be positive integers?

3. **a.** How many 5-digit zip codes can exist where the numbers are in increasing order?

b. How many 5-digit zip codes can exist where the digits are nondecreasing (like 12358 or 03399)?

4. How many ways can you rearrange the letters of "MISSPELLINGS"?

5. How many 9-digit zip codes use one 1, two 2s, three 3s, and three 4s?

Lecture Six
The Principle of Inclusion-Exclusion

Scope: We know from the rule of sum that if A and B are sets with no elements in common, then when we combine these 2 sets, the size of the new set is just the size of A plus the size of B. But what if sets A and B have elements in common? Then elements that appear in both sets are counted twice, so we have to subtract the number of elements that appear in both sets from the size of A plus the size of B. This is the essence of the principle of inclusion-exclusion (PIE), which allows us to answer more difficult questions, like what is the probability that a 5-card poker hand has at least 1 card in each suit?

Outline

I. The principle of inclusion-exclusion (PIE) allows us to answer more difficult questions in combinatorics.

A. Among the numbers 1 through 100, how many of them are multiples of 2, 3, or 5?

B. There are 50 multiples of 2, 33 multiples of 3, and 20 multiples of 5, yet the answer is clearly not $50 + 20 + 33 = 103$. The reason the sum is too large is that some of the numbers are counted more than once. For example, multiples of 6 are counted as multiples of 2 and as multiples of 3.

C. As a simpler example, how many of the numbers 1 through 10 are odd or a multiple of 3? There are 5 odd numbers $\{1, 3, 5, 7, 9\}$ and 3 multiples of 3 $\{3, 6, 9\}$, but the answer is not $5 + 3 = 8$, because the sets overlap.

D. The correct answer is $5 + 3 - 2 = 6$, since the numbers 3 and 9 were double counted.

E. The rule of sum (from Lecture Two) can be stated more accurately using the language of sets.

1. A set is a collection of objects, like $A = \{1, 2, 3\}$, $B = \{2, 3, 5, 8\}$.

2. The union of 2 sets, denoted $A \cup B$, is the set of objects that occur in A or B (or possibly both). In our example, $A \cup B = \{1, 2, 3, 5, 8\}$.

3. The intersection, denoted $A \cap B$, is the set of objects that occur in A and B. In our example, $A \cap B = \{2, 3\}$.

4. If sets A and B have no elements in common, then $A \cap B = \{\ \}$, the empty set, sometimes denoted as ϕ. Such sets are called mutually exclusive or disjoint.

5. The size of a set, denoted $|A|$, is the number of elements in the set A. Here, $|A| = 3$, $|B| = 4$, $|\phi| = 0$.

F. The rule of sum states that if $A \cap B = \phi$, then $|A \cup \mathrm{B}| = |A| + |B|$.

G. This rule can be extended to say for any sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$. This way, everything gets counted exactly once.

II. How many 5-card poker hands have at least 1 card in each suit?

A. Here, $S = \{\text{all 5-card hands}\}$, so $|S| = \binom{52}{5}$.

B. Next we have to subtract hands that are spadeless, heartless, diamondless, or clubless. Letting A_1 be the set of spadeless hands, and so on, we get $|A_1| = \binom{39}{5}$, which gets subtracted 4 times, to account for A_1, A_2, A_3, and A_4.

C. Then we have to add back sets like A_1A_2, for hands that were heartless and spadeless, of which there are $\binom{26}{5}$ hands. This number is added back $\binom{4}{2}$ times (once for each A_iA_j pair).

D. Finally, we have to subtract hands with just 1 suit (of the form $A_iA_jA_k$), of which there are $\binom{4}{3}\binom{13}{5}$ sets.

E. Altogether, the number of such hands is
$$\binom{52}{5} = \binom{4}{1}\binom{39}{5} + \binom{4}{2}\binom{26}{5} - \binom{4}{3}\binom{13}{5}.$$

III. How many ways are there to give 11 distinct candies to 4 children so that each child gets at least 1 candy?

A. Without the restriction, there would be 4^{11} allocations.

B. Subtract off 3^{11} ways where child 1 gets none. Ditto for children 2, 3, and 4.

C. Add back 2^{11} ways where children 1 and 2 get none. Ditto for all other pairs of children.

D. Finally, subtract 1 way where children 1, 2, and 3 get none. Ditto for all other triples of children.

E. Altogether, the number of ways is $4^{11} - 4 \cdot 3^{11} + \binom{4}{2} \cdot 2^{11} - \binom{4}{3}$.

F. This problem was considered in Lecture Three, where the answer was given as $4!S(11, 4)$, where $S(x, y)$ is the Stirling number of the second kind. It follows that

$$S(11, 4) = (4^{11} - 4 \cdot 3^{11} + \binom{4}{2} \cdot 2^{11} - \binom{4}{3})/4!.$$

G. Using summation notation:

$$S(11,4) = \frac{1}{4!}\sum_{j=0}^{4}(-1)^j \binom{4}{j}(4-j)^{11} .$$

H. The same reasoning produces the general formula for Stirling numbers of the second kind:

$$S(x,y) = \frac{1}{y!}\sum_{j=0}^{y}(-1)^j \binom{y}{j}(y-j)^{x} .$$

IV. How many numbers between 1 and 1000 are not divisible by 2, 3, or 5?

A. Beginning with 1000 numbers, we subtract multiples of 2, multiples of 3, and multiples of 5, whose sizes are 500, 333, and 200.

B. Next we add back multiples of (2 and 3), multiples of (2 and 5), and multiples of (3 and 5)—that is, multiples of 6, 10, and 15. There are 166, 100, and 66 of those, respectively.

C. Finally, we subtract off multiples of (2, 3, and 5)—that is, multiples of 30, which there are 33 of.

D. Altogether, our answer is $1000 - 500 - 333 - 200 + 166 + 100 + 66 - 33 = 266$.

E. The same technique can be used to answer the question at the beginning of the lecture: How many numbers between 1 and 100 are not divisible by 2, 3, or 5? The answer is $100 - 50 - 33 - 20 + 16 + 10 + 6 - 3 = 26$.

V. The mixed-up homework problem. How many ways can n homework assignments be returned to n students such that no student gets her own homework back? Call the answer D_n.

A. If there were no restrictions, then there would be $n!$ ways.

B. But we have to subtract $(n-1)!$ of them, where student 1 gets her own homework, and ditto for students 2 through n.

C. Then we have to add back those $(n-2)!$ ways where students 1 and 2 get their own back, as well as for each of the $\binom{n}{2}$ pairs.

D. Then we have to subtract $(n-3)!\binom{n}{3}$ times to account for each triple of student, and so on.

E. Thus,

$$D_n = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots$$

$$= \sum_{k=0}^{n}\binom{n}{k}(n-k)!(-1)^k$$

$$= \sum_{k=0}^{n}\frac{n!}{k!(n-k)!}(n-k)!(-1)^k$$

$$= n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

F. So if n homework assignments are returned at random, the probability that nobody gets her own homework is $D_n/n!$, which equals $1 - 1/1! + 1/2! - 1/3! + 1/4! - \cdots \pm 1/n!$.

G. As n grows, this gets closer and closer to $0.367879\ldots = 1/e$, where e is the exponential number $2.718281828459045\ldots$.

Suggested Reading:

Gross and Harris, *The Magic of Numbers*, chap. 3.

Rosen, *Discrete Mathematics and Its Applications*, chap. 6.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 18.

Tucker, *Applied Combinatorics*, chap. 8.

Questions to Consider:

1. How many numbers between 1 and 100 are not divisible by 3, 4, or 5?

2. How many ways are there to arrange the letters of EXCLUSION that avoid the words SIX and OUNCE?

3. Without using the method of inclusion-exclusion, determine the number of 5-card poker hands that have at least 1 card in each suit. (The answer is simply the product of a few numbers.)

4. Recall that the formula for the number of ways to return n homework assignments to n students such that no student receives his own homework is given by the derangement number $D_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} = n!(1-1/1!+1/2!-1/3!+\cdots\pm 1/n!)$. Verify this formula when n = 1, 2, 3, and 4.

5. How many ways are there to arrange the numbers 1 through 7 so that exactly 3 of them are in their natural positions? (For example, 1432576 has the numbers 1, 3, and 5 in their natural positions.)

Lecture Seven
Proofs—Inductive, Geometric, Combinatorial

Scope: Mathematics is the science of patterns, and discrete mathematics is full of patterns. For example, what do you get when you sum the first n numbers, or the first n odd numbers, or the first n numbers in a row or column or diagonal of Pascal's triangle? Mathematicians confirm these patterns using various proof techniques. One of the most popular proof techniques is called mathematical induction, where you show that if the pattern appears in problems of a given size, then it will continue to work in problems of the next size. Another technique we use is a so-called geometric proof, also sometimes called a proof without words. Patterns can also be proved by counting arguments, known as combinatorial proofs. We illustrate all 3 techniques using Pascal's triangle and the Fibonacci numbers.

Outline

I. Proofs by induction are a fundamental tool in any mathematician's tool kit.

A. What is the sum of the first n odd numbers?

1. The first few sums are 1, 4, 9, 16, 25—perfect squares!

2. It seems reasonable to conjecture that the sum of the first n odd numbers is n^2. That is, for $n \geq 1$,
$1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

3. We can prove this claim by induction.

4. First we prove it true for our base case, $n = 1$.
Certainly, $1 = 1^2$.

5. Next we state our induction hypothesis (called IHOP), where we assume the theorem is true for some particular number k.
Here, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$.

6. Our goal is to prove that it will continue to be true for the number $k + 1$. That is, we wish to show that the sum of the first $k + 1$ odd numbers will be $(k + 1)^2$.

7. To do this, consider the sum $1 + 3 + \cdots + (2k - 1) + (2k + 1)$. We know that, prior to the last summand, the induction hypothesis says that this will sum to k^2. After adding the last term, $2k + 1$, we get $k^2 + 2k + 1$, which is $(k + 1)^2$, as desired.

B. Now use induction to prove that the sum of the first n numbers is $n(n + 1)/2$.

1. Base case: When $n = 1$, $1 = (1)(2)/2$ is true.

2. IHOP: Assume this is true for k: $1 + 2 + \cdots + k = k(k + 1)/2$.

3. Our goal is to show that the first $k + 1$ numbers sum to $(k + 1)(k + 2)/2$.

4. Now, by IHOP, $1 + 2 + \cdots + k + (k + 1) = k(k + 1)/2 + (k + 1)$, which equals $(k + 1)/(k/2 + 1) = (k + 1)(k + 2)/2$, as desired.

C. Many of the patterns in Pascal's triangle can be proved by induction, using Pascal's identity in the induction step. Pascal's identity says $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

II. The Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, … .

A. They are defined by the initial conditions $F_0 = 0$, $F_1 = 1$, and the rule $F_n = F_{n-1} + F_{n-2}$.

B. Let us prove $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$ by induction on n.

1. Base case: When $n = 1$, $F_1 = 1 = F_2$.

2. IHOP: Assume this is true for the number k.

3. Goal: To prove this is true for $k + 1$, we must show that $F_1 + F_3 + \cdots + F_{2k-1} + F_{2k+1} = F_{2(k+1)}$.

4. Using IHOP, the left side equals $F_{2k} + F_{2k+1}$, which equals F_{2k+2}, as desired.

C. Prove that for $n \geq 1$, $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.

1. Base case: When $n = 1$, $F_1^2 = 1 = F_1 F_2$.

2. IHOP: Assume this is true for the number k.

3. Our goal is to prove $F_1^2 + F_2^2 + \cdots + F_k^2 + F_{k+1}^2 = F_{k+1} F_{k+2}$.

4. Inductively, this equals $F_k F_{k+1} + F_{k+1} F_{k+1} = F_{k+1}(F_k + F_{k+1}) = F_{k+1} F_{k+2}$, as desired.

III. Tiling problems highlight an advantage of combinatorial proofs over induction.

A. Consider the combinatorics question: How many sequences of 1s and 2s sum to the number n? Call the answer f_n.

B. Example: $f_4 = 5$, since 4 can be expressed as 2 + 2, or 2 + 1 + 1, or 1 + 2 + 1, or 1 + 1 + 2, or 1 + 1 + 1 + 1.

C. Notice $f_1 = 1, f_2 = 2, f_3 = 3, f_4 = 5$, and $f_5 = 8$. They appear to be Fibonacci numbers. Why?

D. A sum to n can be created 2 ways: as a sum to $n - 1$ followed by a 1 or as a sum to $n - 2$ followed by a 2. Therefore $f_n = f_{n-1} + f_{n-2}$. (We also define $f_0 = 1$.)

E. Equivalently, f_n is the number of ways to tile a strip of length n using squares and dominoes.

F. This tiling interpretation allows many Fibonacci identities to be given a direct combinatorial proof.

G. Prove $(f_{n-1})^2 + (f_n)^2 = f_{2n}$.

1. In a combinatorial proof, we ask a question and answer it 2 ways.

2. Question: How many ways are there to tile a strip of length $2n$?

3. Answer 1: By definition, f_{2n}.

4. Answer 2: There are $(f_n)^2$ tilings of length $2n$ that are breakable in the middle (at cell n). There are $(f_{n-1})^2$ tilings that are not breakable at cell n (since they have a domino covering cells n and $n + 1$). Hence the total number of tilings is $(f_{n-1})^2 + (f_n)^2$, as desired.

H. We note that the above proof is very hard to prove by induction, but the combinatorial proof is clear, and it leads to a natural generalization. By considering whether or not a board of length $m + n$ is breakable at cell m, we get $f_{m+n} = f_m f_n + f_{m-1} f_{n-1}$.

I. To combinatorially prove $f_0 + f_2 + f_4 + f_6 = f_7$, note that a tiling of length 7 must have at least 1 square, and that the last square must be in position 7 or 5 or 3 or 1, preceded by a tiling of length 6 or 4 or 2 or 0.

J. Summing the diagonals of Pascal's triangle leads to the following identity: For $n \geq 0$, $\sum_{k \geq 0} \binom{n-k}{k} = f_n$.

Suggested Reading:

Benjamin and Quinn, *Proofs That Really Count*, chap. 1.

Gross and Harris, *The Magic of Numbers*, chap. 6.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chaps. 2, 4.

Rosen, *Discrete Mathematics and Its Applications*, chap. 3.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 12, 21.

Questions to Consider:

1. Notice that $1 + 2 + 1 = 4$, $1 + 2 + 3 + 2 + 1 = 9$, and $1 + 2 + 3 + 4 + 3 + 2 + 1 = 16$. What pattern do you see? Prove the pattern by induction.

2. Give a geometric proof of the pattern in question 1.

3. Prove by induction: $(1 \times 2) + (2 \times 3) + (3 \times 4) + \cdots + [(n - 1) \times n] = (n - 1)n(n + 1)/3$.

4. The Fibonacci numbers satisfy: $f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$.

a. Prove it by induction.

b. Prove it combinatorially.

Lecture Eight
Linear Recurrences and Fibonacci Numbers

Scope: The Fibonacci numbers have a beautiful formula:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

But how could such a formula have been discovered? Using the roots of a polynomial (in this example, $x^2 - x - 1$), we can find the formula for any quantity defined by a linear recurrence with constant coefficients. The Fibonacci numbers satisfy a second-order recurrence, $F_n = F_{n-1} + F_{n-2}$, since they depend on the previous 2 terms. We will see how recurrences arise naturally in the solution to combinatorial problems and see how the polynomial method for solving recurrences can be extended to handle recurrences of order 3 and higher. We will also be introduced to the Lucas numbers, which grow like the Fibonacci numbers but have different initial conditions. The Lucas numbers interact with the Fibonacci numbers in many interesting ways.

Outline

I. In cases where you are not immediately able to classify a combinatorics problem, the problem will often have a repetitive structure that you will be able to exploit. Let us look at some examples.

A. How many ways can you arrange the numbers 1 through n so that each number is at most 1 away from its original position? Call the answer a_n.

1. For example, $a_3 = 3$ counts 123, 132, and 213.

2. Also notice $a_1 = 1$ and $a_2 = 2$.

3. For $n \geq 3$, a_n satisfies the recurrence $a_n = a_{n-1} + a_{n-2}$, since there are a_{n-1} arrangements where the number n is in the n^{th} position, and there a_{n-2} arrangements where the number n is in position $n - 1$.

B. A cat likes to run down the stairs by going down either 1 step or 3 steps. How many ways can it go down a flight of n steps? Call the answer a_n.

1. This is the same as counting the ways to write the number n as the sum of 1s and 3s.

2. Thus $a_4 = 3$ counts 31, 13, and 111. Also $a_1 = 1$, $a_2 = 1$, and $a_3 = 2$.

3. Since the first step can be size 1 or size 3, this leads to the third-order recurrence $a_n = a_{n-1} + a_{n-3}$.

C. The Fibonacci numbers are defined by initial conditions $F_0 = 0$, $F_1 = 1$, and the second-order recurrence $F_n = F_{n-1} + F_{n-2}$.

1. Fibonacci numbers were first introduced by Leonardo of Pisa in his book *Liber Abaci*. They appeared as an arithmetical exercise that involved the counting of pairs of rabbits.

2. The Fibonacci numbers have a beautiful closed form, known as Binet's formula. For $n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

3. For example, $F_{13} = \frac{1}{\sqrt{5}}[(1.618...)^{13} - (-.618...)^{13}] = 233.$

D. In this lecture, we show why Fibonacci numbers have such a nice closed form and describe a method to solve most k^{th}-order linear recurrences of the form $a_n = p_1 a_{n-1} + p_2 a_{n-2} + \cdots + p_k a_{n-k}$.

II. The solution for the second-order recurrence of the Fibonacci numbers is known as Binet's formula.

A. As we will see, almost every second-order recurrence has a solution of the form $a_n = c_1 r_1^{\,n} + c_2 r_2^{\,n}$.

B. The proof of Binet's formula is by induction.

1. We verify the initial conditions when $n = 0$ and 1.

2. Our induction hypothesis assumes the formula to be true for k and $k - 1$.

3. To prove it for $k + 1$, we use $F_{k+1} = F_k + F_{k-1}$ and then apply the induction hypothesis.

4. To complete the induction, we apply the fact that

$$\phi + 1 = \phi^2 \text{ and } \bar{\phi} + 1 = \bar{\phi}^2, \text{ where } \phi = \frac{1+\sqrt{5}}{2} \text{ and } \bar{\phi} = \frac{1-\sqrt{5}}{2}.$$

5. To summarize, the Fibonacci recurrence $F_n = F_{n-1} + F_{n-2}$ has a closed form $c_1 r_1^n + c_2 r_2^n$, where r_1 and r_2 are roots of the polynomial $x^2 - x - 1$. Note the polynomial's resemblance to the recurrence $F_n - F_{n-1} - F_{n-2} = 0$.

III. The polynomial method for second-order recurrences is the main result of this lecture.

A. Almost any second-order recurrence $a_n = pa_{n-1} + qa_{n-2}$ will have a closed form $c_1 r_1^n + c_2 r_2^n$, where r_1 and r_2 are the roots of $x^2 - px - q$. The constants c_1 and c_2 are determined by the initial conditions.

B. Example: Let $a_0 = 1$; $a_1 = 2$; and for $n \geq 2$, $a_n = a_{n-1} + 6a_{n-2}$.

1. Thus $a_2 = 2 + 6 = 8$, $a_3 = 8 + 6(2) = 20$, $a_4 = 68$, and so on.

2. The recurrence requires us to find roots of the polynomial $x^2 - x - 6 = (x - 3)(x + 2)$, which has roots $r_1 = 3$ and $r_2 = -2$.

3. Thus for all $n \geq 0$, $a_n = c_1 3^n + c_2(-2)^n$.

4. To find c_1 and c_2, let $n = 0$ and $n = 1$; thus, $c_1 + c_2 = a_0 = 1$, and $3c_1 - 2c_2 = a_1 = 2$. Solving these 2 equations in 2 unknowns yields $c_1 = 4/5$ and $c_2 = 1/5$.

5. Thus, our closed form for a_n is $a_n = \frac{4}{5}3^n + \frac{1}{5}(-2)^n$.

C. The polynomial method works even if the roots are complex.

D. The only exception to the polynomial method is when the polynomial has repeated roots. For example, the recurrence $a_n = 4a_{n-1} - 4a_{n-2}$ has polynomial $x^2 - 4x + 4 = (x - 2)^2$.

1. Here a_n has the form $c_1 2^n + c_2 n 2^n$.

2. The constants c_1 and c_2 are determined by the initial conditions.

IV. The polynomial method can be extended to handle higher-order recurrences.

V. Lucas numbers satisfy the same recurrence as the Fibonacci numbers, only with different initial conditions.

A. The Lucas numbers are defined by initial conditions $L_0 = 2$; $L_1 = 1$; and for $n \geq 2$, $L_n = L_{n-1} + L_{n-2}$.

B. Hence the Lucas sequence starts 2, 1, 3, 4, 7, 11, 18, 29, 47, … .

C. The numbers are named after Édouard Lucas (1842–1891), who discovered many beautiful properties of the Fibonacci numbers. He also wrote a classic book on recreational mathematics and developed methods for prime number testing that are still used today.

D. Since the Lucas numbers satisfy the same recurrence as Fibonacci numbers (but with different initial conditions), they have the same polynomial and therefore the same roots. The Binet formula for the Lucas numbers is $L_n = \phi^n + \overline{\phi}^n = (1.618...)^n + (-.618...)^n$.

E. Using the Binet formula for Fibonacci and Lucas numbers, it is easy to prove that $F_n L_n = F_{2n}$.

F. Lucas numbers also have a nice combinatorial interpretation. L_n is the number of ways to tile a circular strip of length n using squares and dominoes.

G. This leads to a simple combinatorial proof that $L_n = f_n + f_{n-2}$, since $f_n = F_{n+1}$ is the number of ways to tile a strip of length n, and f_{n-2} counts those strips that have a domino covering cells n and 1.

Suggested Reading:

Rosen, *Discrete Mathematics and Its Applications*, chap. 6.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 22.

Tucker, *Applied Combinatorics*, chap. 7.

Questions to Consider:

1. Suppose $a_0 = 1$; $a_1 = 11$; and for $n \geq 2$, $a_n = a_{n-1} + 12a_{n-2}$. Generate a_2 and a_3, and then use the polynomial method to find a closed form for a_n.

2. Consider the following game played with a fair 6-sided die: You begin with 3 chips, and you roll the die. If the die shows 1 or 2, you win 1 chip; otherwise, you lose a chip. You keep rolling the die until you either have 5 chips or 0 chips. We wish to determine the probability of reaching 5 chips before 0 chips. (This is an example of the gambler's ruin problem.)

a. To solve this problem, we define a_n to be the probability of reaching 5 chips when you currently have n chips. Our goal is to find a_3, but we will also find a_0, a_1, a_2, a_4, and a_5. Explain why $a_0 = 0$; $a_5 = 1$; and for $n = 1$, 2, 3, and 4, $a_n = (1/3)a_{n+1} + (2/3)a_{n-1}$.

b. Use the polynomial method to solve the recurrence in question (a) above. (Hint: Rewrite the recurrence as $a_{n+1} = 3a_n - 2a_{n-1}$. The polynomial method still works, even though the initial conditions are not consecutive.)

3. Solve the same problem for a fair game, where your chance of winning a chip is 1/2 instead of 1/3. The solution to the recurrence should make intuitive sense.

4. A flagpole of height n can be decorated with 3 types of flags: red flags of height 1 foot (R), white flags of height 2 feet (W), and blue flags of height 2 feet (B).

a. Determine the number of flagpoles that can be created when the height is 0, 1, 2, 3, and 4 feet.

b. Determine a recurrence for the number of flagpoles of height n feet. (Hint: Consider the color of the flag that is on the bottom.)

c. Using the recurrence and initial condition, find a closed form for the number of flagpoles of height n.

5. Find a third-order recurrence. Let $a_0 = 1$; $a_1 = 1$; $a_2 = 7$; and for $n \geq 3$, $a_n = 7a_{n-1} - 14a_{n-2} + 8a_{n-3}$. Find a closed form for a_n. (Time-saving hint: The roots of the polynomial are all small positive integers, and the coefficient associated with the largest root is 1.)

6. Find a third-order recurrence and initial conditions that lead to a closed form $a_n = 3(2^n) - n2^n + 2(-3)^n$.

Lecture Nine

Gateway to Number Theory—Divisibility

Scope: Here we begin our second major theme of discrete mathematics: number theory. We start by developing important properties of numbers, some of which are intuitive, and some of which are surprising. Along the way, we learn how to do rigorous proofs about numbers. To find the greatest common divisor of any 2 numbers, we invoke one of the oldest algorithms in mathematics: Euclid's algorithm. To help us understand the speed of this algorithm, the Fibonacci numbers make a surprise appearance.

Outline

I. Number theory is nicknamed the Queen of Mathematics, suggesting that the subject is both beautiful and pure.

A. The English mathematician G. H. Hardy said that he was interested only in mathematics as a creative art, and he boasted that his work would have no practical applications.

B. Although these lectures on number theory will indeed demonstrate the beauty of number theory, we will also see many applications of it.

C. The positive numbers are 1, 2, 3, 4, … .

1. Appending the number 0 to this list results in the whole numbers.

2. Appending the negative numbers gives us the set of integers: … , −3, −2, −1, 0, 1, 2, 3, … .

D. We shall presume familiarity with basic properties of integers, such as the commutative, associative, and distributive laws.

E. But we shall temporarily prohibit any use of primes, greatest common divisors, or modular arithmetic, until they are properly introduced.

II. Divisibility sheds special light on numbers.

A. We know that when you add, subtract, or multiply integers, you get another integer. But not so with division. When we divide integers, we get a unique quotient and remainder, as described in the division theorem.

B. The division theorem: For positive integers a and d, there are unique integers q and r such that $a = dq + r$, where $0 \leq r < d$.

C. We say that d divides a if there is an integer q such that $a = dq$.

1. Notation: $d|a$.

2. Examples: $3|12$, $2|-6$, and $7|0$.

D. Integer combination theorem: If $d|a$ and $d|b$, then $d|(ax + by)$ for any integers x and y.

III. Greatest common divisors.

A. The number 30 has divisors ±1, ±2, ±3, ±5, ±6, ±10, ±15, and ±30.

1. The numbers 12 and 30 have common divisors ±1, ±2, ±3, ±6.

2. We say that their greatest common divisor is 6, denoted by $\gcd(12, 30) = 6$ or simply as $(12, 30) = 6$.

B. When $(a, b) = 1$, we say that a and b are relatively prime. For example, 16 and 9 are relatively prime.

C. Bézout's theorem: If a and b are relatively prime, then there exist integers x and y so that $ax + by = 1$.

1. The idea of the proof is that given any integer combination $ax + by$ that is bigger than 1, we can always find a new x and y to create a smaller positive integer.

2. Proof: Suppose $ax + by = d > 1$.

3. Since $(a, b) = 1$, d cannot divide both a and b. Say d does not divide a.

4. Then by the division theorem, $a = dq + r$, where $0 < r < d$.

5. But then $r = a - dq = a - (ax + by)q = a(1 - xq) + b(yq)$.

6. Thus r is also an integer combination of a and b, which is smaller than d.

7. Repeating this argument leads to finding an x and y for which $ax + by = 1$.

D. Bézout's theorem generalizes as follows: If $(a, b) = g$, then there exist integers x and y so that $ax + by = g$.

1. Proof: a/g and b/g are relatively prime integers.

2. Thus from our last theorem, there exist x and y so that $(a/g)x + (b/g)y = 1$.

3. Hence $ax + by = g$.

IV. Four of the 13 books of Euclid's *Elements* are devoted to number theory, and Euclid's algorithm for how to find greatest common divisors appeared as the second proposition of book 7 more than 2000 years ago.

A. Euclid's theorem: For any numbers a, b, and x, $\gcd(a, b) = \gcd(b, a - bx)$.

B. When computing (a, b) using Euclid's theorem, it is generally a good idea to try to make x as large as possible. In particular, suppose that $a = bq + r$, where $0 \le r < b$. Setting $x = q$, we get $(a, b) = (b, a - bq) = (b, r)$. And since $r = a \bmod b$, we have a very efficient algorithm.

C. Euclid's algorithm: $(a, b) = (b, a \bmod b)$.

1. Example: $(53, 10) = (10, 53 \bmod 10) = (10, 3) = (3, 10 \bmod 3) = (3, 1) = (1, 3 \bmod 1) = (1, 0) = 1$.

2. More compactly: $(53, 10) = (10, 3) = (3, 1) = (1, 0) = 1$.

D. Euclid's algorithm is fast. If $a > b$, then the algorithm will find (a, b) in under $5 \log_{10} b$ steps. So if a and b are 100-digit numbers, then Euclid finds $\gcd(a, b)$ in under 500 steps.

E. Which 2-digit numbers will require the most steps from Euclid's algorithm? The Fibonacci numbers.

Suggested Reading:

Benjamin and Brown, *Biscuits of Number Theory*.

Dudley, *Elementary Number Theory*, sec. 1.

Gross and Harris, *The Magic of Numbers*, chap. 8.

Hardy and Wright, *An Introduction to the Theory of Numbers*.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 6.

Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*, chap. 1.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 34–35.

Silverman, *A Friendly Introduction to Number Theory*, chaps. 5–6.

Questions to Consider:

1. Can every integer be expressed in the form $12x + 27y$, where x and y are integers?
2. Can every integer be expressed in the form $13x + 27y$, where x and y are integers?
3. Use Euclid's algorithm to find the greatest common divisor of 133 and 91.
4. Express the answer to question 2 in the form $133x + 91y$.
5. Which Fibonacci numbers are even? Can you prove your answer?

Lecture Ten
The Structure of Numbers

Scope: In this lecture, we explore the building blocks of the integers. Numbers can be created additively or multiplicatively. Every number can be expressed as the sum of distinct powers of 2 in a unique way. This convenient way to represent numbers is known as binary notation. The multiplicative building blocks of the integers are the prime numbers. There are still many interesting unsolved problems about prime numbers.

Outline

I. Powers of 2 form a particularly nice set of additive building blocks for the positive integers, known as binary representation.

- **A.** Every positive number can be expressed as the sum of powers of 2 in a unique way. For example, $83 = 64 + 16 + 2 + 1$. We represent this using binary notation by saying $83 = (1010011)_2$, indicating that $83 = 64(1) + 32(0) + 16(1) + 8(0) + 4(0) + 2(1) + 1(1)$.
- **B.** This can be proved using a technique called strong induction.

II. The prime numbers form an especially nice set of multiplicative building blocks.

- **A.** A positive number is prime if it has exactly 2 positive divisors, 1 and itself.
  1. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, … .
  2. A positive number with 3 or more divisors is composite.
  3. The number 1 is neither prime nor composite. It is called a unit.
- **B.** Every number can be factored into primes.
- **C.** Important theorem: If $d|ab$ and $(d, a) = 1$, then $d|b$.
  1. Proof: Since $d|ab$, then $ab = dq$ for some integer q.
  2. Since $(d, a) = 1$, $dx + ay = 1$ for some x and y.
  3. Thus, $dbx + aby = b$, and since $ab = dq$, this says that $dbx + dqy = b$.
  4. But then $d(bx + qy) = b$, and therefore $d|b$.

D. Theorem of prime importance: Let p be prime. If $p|ab$, then $p|a$ or $p|b$.

1. Proof: Suppose $p|ab$. If $p|a$, then we are done.

2. Otherwise, $(p, a) = 1$ (since p has only 2 divisors, p and 1).

3. Hence by the important theorem, $p|b$.

4. Either way, $p|a$ or $p|b$.

E. This theorem can be extended using induction to prove that if $p|a_1a_2\ldots a_n$, then $p|a_1$ or $p|a_2$ or $\ldots$ $p|a_n$. This theorem will be used in our proof of the fundamental theorem of arithmetic.

III. The fundamental theorem of arithmetic (also known as the unique factorization theorem) says that every positive number has a unique factorization into prime numbers.

A. The first half of the fundamental theorem says that every number $n \geq 2$ can be factored into primes.

B. The second half of the fundamental theorem says that every number $n \geq 2$ can be factored into primes in a unique way.

C. By the fundamental theorem, every positive number is of the form $n = 2^{e_1}3^{e_2}5^{e_3}7^{e_4}11^{e_5}\cdots$ where $e_i \geq 0$ for all i. For example, $280 = 2^3 3^0 5^1 7^1$ or $280 = 2^3 5^1 7^1$.

D. If you know how a number factors, then you know a lot about the number.

1. The number n is a perfect square if and only if every exponent is even.

2. If $d = n = 2^{f_1}3^{f_2}5^{f_3}7^{f_4}11^{f_5}\cdots$, then d is a divisor of n if and only if $f_i \leq e_i$ for all i.

3. Hence the number of divisors of n is $(1 + e_1)(1 + e_2)(1 + e_3)\ldots$, since the power of 2 must be some number between 0 and e_1, the power of 3 must be between 0 and e_2, and so on. For example, $126 = 2^1 3^2 7^1$ has $2 \times 3 \times 2 = 12$ positive divisors.

4. If $a = 2^{a_1}3^{a_2}5^{a_3}7^{a_4}11^{a_5}\cdots$ and $b = 2^{b_1}3^{b_2}5^{b_3}7^{b_4}11^{b_5}\cdots$, then $\gcd(a, b)$ can be obtained by using the minimum of each exponent. For example, if $a = 126 = 2^1 3^2 5^0 7^1$, and $b = 600 = 2^3 3^1 5^2 7^0$, then $\gcd(a, b) = 2^1 3^1 5^0 7^0 = 6$.

5. Replacing min with max produces the least common multiple of a and b, denoted $\text{lcm}(a, b)$ or $[a, b]$.

6. These facts combine to show that $(a, b)[a, b] = ab$.

IV. The behavior of prime numbers is both regular and irregular.

A. There are infinitely many prime numbers, and yet there are arbitrarily long strings of consecutive composite numbers.

B. There are infinitely many primes of the form $4k + 1$, and there are infinitely many primes of the form $4k + 3$. In fact, Dirichlet proved that there are infinitely many primes of the form $ak + b$, whenever $(a, b) = 1$.

C. Yet we do not know if there are infinitely many primes of the forms $x^2 + 1$, $2^n + 1$, $2^n - 1$, $10^n + 1$, or $n! + 1$.

D. Nor do we know if there are infinitely many twin primes, primes consisting of all 1s, or prime Fibonacci numbers.

E. Despite the irregularity of primes, when you look at them from a distance, there is a discernible pattern.

Suggested Reading:

Dudley, *Elementary Number Theory*, sec. 2.

Gross and Harris, *The Magic of Numbers*, chaps. 10–11, 23.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 6.

Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*, chap. 1.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 38.

Silverman, *A Friendly Introduction to Number Theory*, chap. 7.

Young, *Excursions in Calculus*, chap. 5.

Questions to Consider:

1. Express the number 57 as the sum of distinct powers of 2 and give its binary representation.

2. Provide the prime factorization of 2520.

3. How many positive divisors does 2520 have?

4. Using the prime factorization of 825, find the greatest common divisor and the least common multiple of 2520 and 825.

5. Prove that if a number is the sum of 2 squares, it cannot be a Gaussian prime. Use this to show that the prime numbers 17 and 109 are not Gaussian primes, and find a way to factor them into complex numbers.

Lecture Eleven

Two Principles—Pigeonholes and Parity

Scope: The pigeonhole principle says that if $n+1$ objects are placed into n containers, then there must exist a container with at least 2 objects. From this very simple idea, we can solve many complex-sounding mathematical problems. The parity principle allows us to figure out many mathematical conundrums by simply keeping track of odd and even numbers. These can be used to prove that certain mathematical constructions are impossible. Parity can be used to provide an efficient means of error detection for transmitted binary code words.

Outline

I. The pigeonhole principle says that if $n + 1$ objects are placed into n boxes, then some box must contain 2 or more objects.

A. For example, if you choose 5 cards from a deck, then since there are only 4 different suits, 2 of those cards must be of the same suit.

B. The generalized pigeonhole principle says that if $pn + 1$ or more objects are placed into n boxes, then some box has at least $p + 1$ objects.

1. Proof by contradiction: Suppose that each box has at most p objects. Then the total number of objects would be at most pn, contradicting our assumption.

2. Example: If 17 yellow pigs are placed into 5 giant holes, then since 17/5 = 3.4, some hole must have at least 4 pigs. (You might call this the pig-in-hole principle!)

C. Claim: If 5 points are chosen inside a 2 × 2 square, then there must be 2 points within $\sqrt{2}$ of each other.

1. Proof: To see this, divide the square into four 1 × 1 quadrants. By the pigeonhole principle, 2 points must be in the same quadrant.

2. The distance between 2 points in the same quadrant is at most the length of the diagonal from one corner to the other, which is (by the Pythagorean theorem) $\sqrt{2}$.

II. We can see how the pigeonhole principle works with examples from number theory.

A. Claim: There are 2 powers of 3 whose difference is divisible by 2009.

1. Proof: Consider the 2010 numbers $3^1, 3^2, 3^3, \ldots, 3^{2010}$.

2. Divide each number by 2009, and look at the remainder.

3. Since there are only 2009 possible remainders (0 through 2008), 2 of them must have the same remainder r.

4. Thus for some exponents x and y (where we assume that x is greater than y), $3^x = 2009q_1 + r$, and $3^y = 2009q_2 + r$.

5. Subtracting yields $3^x - 3^y = 2009(q_1 - q_2)$.

6. Thus 2009 divides $3^x - 3^y$.

7. Note that the proof does not tell us how to find x and y, but it proves that they must exist.

B. Claim: There is a positive power of 3 that ends in 001.

1. By the same argument as above, we know there exist $0 < y < x \leq 1000$, so that 1000 divides $3^x - 3^y = 3^y(3^{x-y} - 1)$.

2. Notice that $\gcd(1000, 3^y) = 1$, so by the important theorem, 1000 divides $3^{x-y} - 1$.

3. Thus $1000q = 3^{x-y} - 1$ for some integer q.

4. Thus $3^{x-y} = 1000q + 1$ ends in 001.

5. Again, the proof does not tell us what the exponent is, only that it must exist.

III. The parity principle involves keeping track of odd and even numbers.

A. While the pigeonhole principle is often used to prove that some sort of mathematical situation is inevitable, the parity principle is often used to prove that certain outcomes are impossible.

B. Definition: If n is a multiple of 2 (that is, n is of the form $2q$), then the parity of n is even. Otherwise (n is of the form $2q + 1$), the parity of n is odd.

C. Question: Is it possible to fill in the blanks below with + and − signs to create a total of 20?

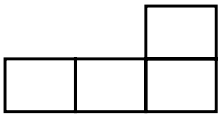
1 _ 2 _ 3 _ 4 _ 5 _ 6 _ 7 _ 8 _ 9

1. No. Since we have 5 odd numbers, the final total must be odd.

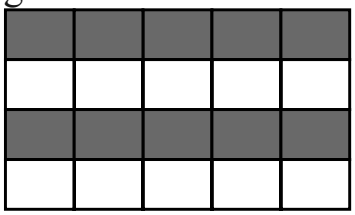
2. Why? Each time we add or subtract an odd number, the parity will change (whereas adding or subtracting an even number leaves the parity unchanged).

3. Since the parity of the total is odd, it cannot be 20.

D. Question: Is it possible to cover a 4 × 5 grid (containing 20 squares) with 5 nonoverlapping L-shaped tiles that look like this?



1. We show that this is impossible by coloring the rows of the grid as follows.



2. Notice that anywhere you place an L-shaped tile, it covers either 3 dark squares or 1 dark square. But we have 10 dark squares that need to be covered using 5 tiles. This is impossible since 5 odd numbers cannot sum to 10.

E. If a code word consists of n 0s and 1s, then we know there are 2^n possible code words. For example, when $n = 3$, the 8 code words are 000, 001, 010, 011, 100, 101, 110, and 111.

F. But if 2 code words are too similar, then they can be confused if a 0 turns into a 1 or vice versa. By reducing the number of code words, we can detect single-digit errors.

G. The parity check method uses only code words that have an even number of 1s. This can detect if a code word has 1 digit incorrect. When $n = 3$, the code words are 000, 011, 101, and 110. In general, the number of code words of length n with an even number of 1s is 2^{n-1}.

H. Is error detection possible with more than 2^{n-1} code words?

1. No, since each code word can be paired up with its mate, which is identical except for the first digit.

2. In general, there are 2^{n-1} couples. Thus, if the number of code words exceeded 2^{n-1}, it would contain both members of some couple and be susceptible to single-digit errors.

Suggested Reading:

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 2.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 24.

Questions to Consider:

1. A drawer contains a bunch of unpaired socks, which come in 10 different colors. How many socks do you have to remove before you can be guaranteed of at least 1 matching pair?
2. Fill in the blank with the largest number that makes the statement true. In a room with 40 people, there must be at least ____ people who are born in the same month.
3. Use the pigeonhole principle to show that in any set of 51 positive numbers below 100, there must be 2 numbers in the set that sum to 100. Why is the statement false if we replace 51 with 50?
4. Suppose you have a collection of 25 coins, where some of the coins are pennies, nickels, and quarters. Why is it impossible for their grand total to be $5.00?

Lecture Twelve
Modular Arithmetic—The Math of Remainders

Scope: Many problems in number theory can be understood using modular arithmetic, the mathematics of remainders. We say that a and b are congruent modulo m, or $a \equiv b \pmod{m}$, if a and b differ by a multiple of m. For example, when you look at a clock, you are really working mod 12, since 2 times that differ by a multiple of 12 look the same on a clock. In this lecture, we show that the congruence relation behaves a lot like equality. You can add, subtract, and even multiply congruences, but you have to be a little careful with division. We look at several applications of modular arithmetic.

Outline

I. Modular arithmetic is the mathematics of remainders.

A. Modular arithmetic was invented by Carl Friedrich Gauss (1777–1855), in his book *Disquisitiones Arithmeticae*.

B. Definition: For $m > 0$, we say that $a \equiv b \pmod{m}$ if $m|(a - b)$.

1. We read this as "a is congruent to b mod m if m divides $a - b$." The number m is called the modulus.

2. Equivalently, a and b differ by a multiple of m.

3. Equivalently, $a = b + mj$ for some integer j, or a and b have the same remainder when divided by m.

4. Equivalently, $a \bmod m = b \bmod m$.

5. Examples: $26 \equiv 20 \pmod{3}$ since $3|(26 - 20)$. Also $26 \equiv 2$ and $26 \equiv -1 \pmod{3}$, since $3|(26 - 2)$ and $3|[26 - (-1)]$.

C. We have known modular arithmetic ever since we could tell time or read a calendar.

1. A standard 12-hour clock is working mod 12.

2. Calendars operate mod 7, since the day of the week repeats every 7 days.

D. The congruence relation acts a lot like the equality relation.

II. Congruences resemble equality and are central to modular arithmetic.

A. Congruences can be added: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

1. Proof: Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

2. Then m divides $a - b$ and $b - c$ and therefore divides their sum.

3. Thus m divides $(a - b) + (c - d) = (a + c) - (b + d)$.

4. Thus $a + c \equiv b + d \pmod{m}$.

B. Congruences can be multiplied: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

1. Proof: We are given that $a = b + jm$ for some integer j and $c = d + km$ for some integer k.

2. Thus $ac = (b + jm)(d + km) = bd + bkm + jmd + jkm^2 = bd + m(bk + jd + jkm)$.

3. Thus $ac \equiv bd \pmod{m}$.

C. Multiplying the congruence $a \equiv b$ by itself as many times as we want gives us the power theorem: If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for any exponent $n \geq 0$.

III. How can you check the answer to big arithmetic problems by summing the digits of your answer? Why does the method of "casting out 9s" work?

A. For a positive integer x, define $S(x)$ to be the sum of the digits of x. For example, $S(4688) = 26$.

B. Claim: For any $x > 0$, $x \equiv S(x) \pmod{9}$. For example, $4688 \equiv 26 \equiv 8 \pmod{9}$.

1. Idea of proof: $4688 = 4(10^3) + 6(10^2) + 8(10) + 8$.

2. Since $10 \equiv 1 \pmod{9}$, then by the power theorem, this is congruent to $4(1^3) + 6(1^2) + 8(1) + 8 = 26 \pmod{9}$.

C. This theorem can be exploited to do something called casting out 9s as a means of checking addition, subtraction, and multiplication problems.

1. For example, to check the multiplication problem $49 \times 41 = 2009$, reduce the numbers mod 9 (by summing their digits).

2. Note that $49 \equiv 4$, $41 \equiv 5$, and $2009 \equiv 2 \pmod{9}$—and indeed, $4 \times 5 = 20 \equiv 2 \pmod{9}$.

3. This does not guarantee that the multiplication is right, but if they did not match up, then you definitely made a mistake somewhere.

D. Casting out 11s: You can tell if a number is a multiple of 11 by alternately adding and subtracting its digits from right to left.

1. For example, $1234 \equiv 4 - 3 + 2 - 1 = 2 \pmod{11}$.

2. $87 \equiv 7 - 8 = -1 \equiv 10 \pmod{11}$.

3. Why does this work? Since our base 10 is congruent to $-1 \pmod{11}$, $10^k \equiv (-1)^k$.

4. Thus $1234 = 1(1000) + 2(100) + 3(10) + 4 \equiv 1(-1) + 2(1) + 3(-1) + 4 = 2$.

IV. Every book has an ISBN, and that number is coded using mod-11 arithmetic.

A. The ISBN is a 10-digit number *a-bcdef-ghi-j* satisfying the following:

$$10a + 9b + 8c + 7d + 6e + 5f + 4g + 3h + 2i + j \equiv 0 \pmod{11}.$$

B. The last digit, j, is called the check digit, which is used to ensure that the above sum is 0 (mod 11). If j needs to be 10, then it is coded with symbol X.

C. Example: The ISBN of the Lecture Transcript and Course Guidebook for *The Joy of Mathematics* is 1-59803-311-5. We confirm that it is a valid ISBN by dotting the vector (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) with the vector (1, 5, 9, 8, 0, 3, 3, 1, 1, 5) to get $10 + 45 + 72 + 56 + 0 + 15 + 12 + 3 + 2 + 5 = 220 \equiv 0 \pmod{11}$.

D. The advantage of this system is that it can detect an error where 1 digit is incorrectly written or errors resulting from any 2 digits being transposed.

V. We can add, subtract, and multiply both sides of a congruence—but can you divide? Sometimes, as the cancellation theorem indicates.

A. The cancellation theorem: If $ax \equiv ay \pmod{m}$, and if $\gcd(a, m) = 1$, then $x \equiv y \pmod{m}$.

1. Proof: Since $ax \equiv ay \pmod{m}$, then $m|(ax - ay) = a(x - y)$.

2. And since $(a, m) = 1$, then by the important theorem, m divides $x - y$.

3. Thus $x \equiv y \pmod{m}$.

B. We say that the number a has a (multiplicative) inverse mod m if there is some integer x such that $ax \equiv 1 \pmod{m}$.

C. Theorem: The number a has a multiplicative inverse mod m if and only if $(a, m) = 1$. The inverse is unique in the sense that if $ax \equiv 1$ and $ay \equiv 1$, then $x \equiv y \pmod{m}$.

1. The idea of the proof is that a and m are relatively prime if and only if there are integers x and q for which $ax + my = 1$. But then x is an inverse of $a \pmod{m}$.

2. As for uniqueness, if $ax \equiv 1$ and $ay \equiv 1 \pmod{m}$, then $ax \equiv ay \pmod{m}$.

3. But since $(a, m) = 1$, then by the cancellation theorem, $x \equiv y \pmod{m}$.

D. The cancellation theorem can be used to derive Wilson's theorem: n is prime if and only if $(n - 1)! \equiv -1 \pmod{n}$.

Suggested Reading:

Dudley, *Elementary Number Theory*, sec. 4.

Gross and Harris, *The Magic of Numbers*, chaps. 15–16.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 6.

Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*, chap. 2.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 36.

Silverman, *A Friendly Introduction to Number Theory*, chap. 8.

Questions to Consider:

1. **a.** What modulus would you use to determine the month it will be 100 months from now?

b. What modulus would you use to determine the last 2 digits of the number 31,415 plus your 5-digit zip code?

2. Without using a calculator, determine $31{,}415 \times 12{,}358 \pmod{9}$.

3. Do the same problem in question 2, working mod 11.

4. The book *Secrets of Mental Math* has ISBN 0-307-33840-C, where C is the check digit. Determine the digit C.

5. Find the positive numbers below 14 that are relatively prime to 14, and then determine their multiplicative inverses.

Lecture Thirteen
Enormous Exponents and Card Shuffling

Scope: In this lecture, we discuss many applications of modular arithmetic. We begin with the Chinese remainder theorem. We then look at public key cryptography, where it is important to be able to raise large numbers to enormous powers. At first glance, there appears to be no shortcut to doing this, but with the method of successive squaring, it can be done very efficiently. Another application of this idea is the mathematics of perfect shuffles, where a deck is cut exactly in half and the cards are interleaved perfectly.

Outline

I. The Chinese remainder theorem shows that every number between 1 and m_1m_2, where m_1 and m_2 are relatively prime, creates a distinct fingerprint when viewed mod m_1 and mod m_2.

A. Observe that 83 mod 9 = 2 and 83 mod 11 = 6. This theorem will show us that there are no other numbers between 1 and 100 with this property, and that every number between 1 and 99 has a distinct "fingerprint" mod 9 and 11. In other words, the system of congruences, $N \equiv 2 \pmod 9$ and $N \equiv 6 \pmod{11}$ has a unique solution mod 99, namely, $N \equiv 83 \pmod{99}$.

B. The Chinese remainder theorem: If m_1 and m_2 are relatively prime, then the system of congruences $N \equiv a_1 \pmod{m_1}$, $N \equiv a_2 \pmod{m_2}$ has a unique solution mod m_1m_2.

C. Since $(m_1, m_2) = 1$, there exist x and y so that $m_1x + m_2y = 1$, which can be found using Euclid's algorithm.

D. A solution to the system of congruences can be given by the "max + may" formula: $N = m_1a_2x + m_2a_1y$.

E. Proof of the Chinese remainder theorem.

1. Working mod m_1, $N = m_1a_2x + m_2a_1y \equiv m_2a_1y = a_1m_2y = a_1(1 - m_1x) \equiv a_1(1) = a_1 \pmod{m_1}$.

2. Similarly, $N \equiv a_2 \pmod{m_2}$.

3. As for uniqueness, if there were another solution, say N^*, with $N^* \equiv a_1 \pmod{m_1}$ and $N^* \equiv a_2 \pmod{m_2}$, then $N^* \equiv N \pmod{m_1}$ and $N^* \equiv N \pmod{m_2}$, so that m_1 divides $N^* - N$ and m_2 divides $N^* - N$.
4. But since m_1 and m_2 are relatively prime, $m_1 m_2$ divides $N^* - N$, and therefore $N^* \equiv N \pmod{m_1 m_2}$.

II. In a perfect shuffle, the 52 cards are cut exactly in half, then the cards are interlaced perfectly.

A. We number the cards from top to bottom, 0 to 51.

B. In an outshuffle, the cards are rearranged so that card 0 stays on top, followed by card 26, then card 1, then card 27, and so on. It is called an outshuffle because the outermost cards (0 and 51) stay on the top and bottom.

C. In an inshuffle, card 26 goes on top, then card 0, then card 27, then card 1, and so on.

D. Outshuffles have a nice mathematical description. The card at position x is sent to position $O(x) = 2x \pmod{51}$, with the exception that $O(51) = 51$.

E. It takes 8 outshuffles, but 52 inshuffles, to restore the deck.

F. Discrete magic: How do you send the top card to any position n?
1. Express n in binary and follow the instructions!
2. For example, $n = 41 = 32 + 8 + 1 = (101001)_2$ says that your sequence of shuffles should be in-out-in-out-out-in.
3. The reason that this will always work is based on a technique I call seed planting, which is used for raising big numbers to big powers.

III. A naive method of raising numbers to big powers (e.g., $3^{1,000,000}$ or 3 to a 1000-digit number) would take a million multiplications for the former and effectively forever for the latter, but a smart method for those same examples takes only a few dozen or a few hundred multiplications.

A. You can compute 6^{83} in far fewer than 83 multiplications by successive squaring.
1. First compute $6, 6^2, 6^4, 6^8, 6^{16}, 6^{32}$, and 6^{64}.
2. Then $6^{83} = 6^{64}6^{16}6^2 6^1$.

B. For a more streamlined approach, you can do the method of seed planting. Counting down 64, 32, 16, 8, 4, 2, 1, you successively square the number but multiply it by an extra factor of 6 at stages 16, 2, and 1. For example, $6 \rightarrow 6^2 \rightarrow 6^4 6 = 6^5 \rightarrow 6^{10} \rightarrow 6^{20} \rightarrow 6^{40} 6 = 6^{41} \rightarrow 6^{82} 6 = 6^{83}$.

C. The same calculation can be done mod m by reducing the answer mod m at each step. For example, it can be shown that $6^{83} \bmod 79 = 34$.

D. The seed planting method is a fast, all-purpose method. But sometimes we get lucky and can compute $a^n \pmod{m}$ even faster if we can find an exponent d for which $a^d \equiv 1 \pmod{m}$.

Suggested Reading:

Dudley, *Elementary Number Theory*, sec. 5.

Gross and Harris, *The Magic of Numbers*, chap. 18.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 6.

Morris, *Magic Tricks, Card Shuffling*.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 37.

Questions to Consider:

1. What is the smallest number divisible by all of the numbers from 1 through 12?

2. When a marching band tries to line up in rows of 13, it has 3 musicians left over. When it tries to line up in rows of 17, it has 8 musicians left over. If the band has fewer than 100 musicians, how many musicians are in the band?

3. What would be the smallest band size that would satisfy the conditions of the previous problem and also have 1 musician left over when the band lines up in rows of size 7?

4. **a.** Suppose you had a deck of 22 cards. Show that after 6 outshuffles, the deck would be back to its original order.

b. Find the largest number of cards for which 4 outshuffles would return the deck to its original order.

5. Show that $3^{91} \bmod 91 = 3$. As we will learn in the next lecture, if p is a prime number, then $a^p \bmod p = a$. This example illustrates that this is sometimes also true for composite exponents, since $91 = 7 \times 13$.

Lecture Fourteen
Fermat's "Little" Theorem and Prime Testing

Scope: In this lecture, we apply modular arithmetic to discover more peculiar properties of primes, leading to a practical way to test whether a number is prime without trying to factor it. We explore one of the most important theorems in number theory, due to Fermat, which says that if p is prime, then $a^p \equiv a \pmod{p}$. As a consequence of this theorem, if we are given a large number n and we find that n does not divide $2^n - 2$, then n cannot possibly be prime, even though we do not know any of the proper divisors of n. We will also prove a generalization of Fermat's theorem, due to Euler, which forms the basis of public key cryptography.

Outline

I. Pierre de Fermat (1601–1655) was one of the most important mathematicians of his time.

A. He was employed as a lawyer, not a professional mathematician.

B. Fermat was brilliant at discovering beautiful mathematical patterns. He usually did not prove his discoveries but would share them with other mathematicians for them to prove.

C. His most famous unsolved problem became known as Fermat's last theorem, which says that for $n \geq 3$, it is impossible to find 3 positive integers a, b, c, such that $a^n + b^n = c^n$.

1. Fermat actually proved this when $n = 4$, and Euler later proved it when $n = 3$.

2. Fermat wrote his last theorem in the margins of his copy of the book *Arithemetica* by Diophantus.

3. It took more than 350 years before a correct proof was given, by Andrew Wiles in 1995.

D. Fermat also investigated properties of perfect numbers. A number is perfect if it is the sum of its proper divisors.

1. For example, 6 and 28 are perfect since $6 = 1 + 2 + 3$, and $28 = 1 + 2 + 4 + 7 + 14$.

2. Euclid proved that if a number is of the form $x = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime, then x is perfect.

3. Thus Fermat was motivated to answer the question "When is $2^n - 1$ prime?"

II. Fermat discovered his so-called little theorem while investigating perfect numbers.

A. Fermat's little theorem: For any integer a and any prime number p, $a^p \equiv a \pmod{p}$.

B. Before we prove Fermat's theorem, let's say a few words about logic. The theorem "If p, then q" is logically equivalent to the theorem "If not q, then not p." This is called the contrapositive theorem, and you get it for free.

C. On the other hand, "If p, then q" is not the same as "If q, then p." That is called the converse statement and needs separate proof, if it is even true at all.

D. We use a contrapositive version of the cancellation theorem to prove Fermat's little theorem.

III. While Fermat's theorem concerned any prime modulus, Euler's generalization extended to any composite modulus.

A. Leonhard Euler (1707–1783) made profound contributions to all areas of mathematics, including combinatorics, number theory, and graph theory. Here, we show how Euler generalized Fermat's theorem to composite moduli.

B. For $m \geq 1$, we let $\phi(m)$ be the number of numbers in $\{1, 2, \ldots, m\}$ that are relatively prime to m.

1. Example: $\phi(10) = 4$ counts the numbers 1, 3, 7, 9.
2. Example: For p prime, $\phi(p) = p - 1$ counts $1, 2, \ldots, p - 1$.

C. Fermat's theorem says that if p is prime, then $a^p \equiv a \pmod{p}$. When $(a, p) = 1$, we can divide both sides by a to get $a^{p-1} \equiv 1 \pmod{p}$.

D. Euler's generalized theorem: Let $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

1. Proof [supplemental to the lecture]: Let $S = \{r_1, r_2, \ldots, r_t\}$ be the numbers below m that are relatively prime to m.
2. Thus $t = \phi(m)$, by the definition of $\phi(m)$.
3. Just like in the proof of Fermat's theorem, $aS = \{ar_1, ar_2, \ldots, ar_t\} \equiv \{r_1, r_2, \ldots, r_t\} \pmod{p}$.

4. Multiplying the elements of both sets, $a^t r_1 r_2 \cdots r_t \equiv r_1 r_2 \cdots r_t \pmod{p}$.
5. Since each r_i is relatively prime to p, the cancellation theorem gives the desired result: $a^t \equiv 1 \pmod{p}$.

IV. Fermat's theorem offers an imperfect test for compositeness.

A. Fermat's theorem can be stated as follows: If n is prime, then $a^n \equiv a \pmod{n}$.

B. The contrapositive of Fermat's theorem says that if a^n is not congruent to $a \pmod{n}$, then n is not prime. This is called the Fermat primality test.

C. Alas, there are some composite numbers that fool the Fermat test. For example, $2^{341} \equiv 2 \pmod{341}$, even though $341 = 31 \times 11$ is composite.

D. But the composite number $561 = 3 \times 11 \times 17$ is especially stubborn in that $a^{561} \equiv a \pmod{561}$ for every base a. Such numbers are called Carmichael numbers.

Suggested Reading:

Dudley, *Elementary Number Theory*, sec. 6.

Gross and Harris, *The Magic of Numbers*, chaps. 18, 20.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 6.

Scheinerman, *Mathematics: A Discrete Introduction*, sec. 42.

Silverman, *A Friendly Introduction to Number Theory*, chaps. 9–11.

Questions to Consider:

1. The numbers x and y are called amicable if the proper divisors of x sum to y and the proper divisors of y sum to x. Show that 220 and 284 are amicable.

2. Suppose that $x = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is a prime number p. List all the divisors of x (including x itself). Show that x is perfect by verifying that the sum of all the divisors of x is $2x$.

3. Another theorem named after Fermat (sometimes called Fermat's great theorem) says, "Let p be an odd prime. If $p \equiv 1 \pmod{4}$, then p is the sum of 2 squares." State the contrapositive of this theorem. State the converse of the theorem, and prove that it is also true.

4. Without using a calculator, determine $2^{100} \bmod 101$. How about $2^{703} \bmod 101$?

5. Compute the number of positive numbers below 2520 that are relatively prime to 2520. Use your answer to find an exponent e for which $11^e \equiv 11 \bmod 2520$.

Lecture Fifteen

Open Secrets—Public Key Cryptography

Scope: Suppose that to encode a secret message, you take every letter of your message and shift the letter forward by 3 letters. For instance, the word CAT would become FDW. Then when someone receives the secret message, it is a simple matter to reverse the procedure by shifting each letter backward by 3 letters. With public key cryptography, however, everyone knows how the messages get encoded, yet only the recipient knows how to reverse the procedure. This idea is one of the ways Internet commerce remains secure. We will explore the RSA method for doing public key cryptography.

Outline

I. Public key cryptography (from the Greek roots "crypto" and "graphon," meaning "hidden writing") is perhaps the most discreet application of discrete mathematics.

A. Suppose I have a secret message that I want to send to you, say, "quiz today." This message is known as the plaintext since it could be read plainly by anyone. How can we disguise our message?

B. One of the simplest codes to create (and break) is the shift method, where every letter is shifted by the same amount. For example if the amount of our shift (known as the key) was to shift every letter forward by 2 (mod 26), then "quiz today" would become "swkb vqfca," known as the ciphertext.

C. Someone reading the ciphertext could not easily determine the plaintext. But if the recipients know the key, they can easily determine the plaintext by shifting every letter backward by 2.

D. The idea behind public key cryptography sounds impossible. Imagine that a bank wants anyone in the world to be able to communicate with it over the Internet in a secure way. The bank posts on its website, for everyone to see, a public key.

E. Here is how it works: On the privacy of your computer, you convert the plaintext into ciphertext using the bank's public key. Then you e-mail the ciphertext to the bank (very insecure). But despite the fact that everyone knows the public key, only the bank can decipher the message.

II. The most famous method for public key cryptography is called the RSA method.

A. It was named after 3 mathematically trained computer scientists, Ronald Rivest, Adi Shamier, and Leonard Adleman, who discovered this method in 1977.

B. Let a, b, and n be enormous numbers (say 2000 digits long). It is very easy for a computer to calculate $a^b \bmod n$ and $\gcd(a, b)$ and to determine if n is a prime number. But if n is composite—say, $n = pq$, where p and q are 1000-digit primes—then it is very hard for a computer to factor n.

C. Here is how RSA works: The bank publishes 2 numbers on its website, n and e (as in "encipher"); n and e are about 2000 digits long.

1. Write your plaintext (under 1000 characters). Example: plaintext = QuizToday.

2. Covert plaintext to a number M (under 2000 digits) by replacing each letter with its 2-digit position in the alphabet. For example, QuizToday becomes 1721092620150401 25.

3. Computer ciphertext $C = M^e \bmod n$. You e-mail C to the bank.

4. When the bank receives C, it uses a magic secret number d (as in "decipher") and computes $C^d \bmod n$, which (amazingly) equals M. Then it converts M back to plaintext.

D. How are d, e, and n chosen?

1. The bank secretly chooses 2 random 1000-digit primes, p and q, and computes $n = pq$. The product n is made public, but the primes p and q are kept private.

2. The bank computes $\phi(n) = (p - 1)(q - 1)$, then selects a random 1000-digit number d that is relatively prime to $\phi(n)$, using the Euclidean algorithm.

3. Since $(d, \phi(n)) = 1$, Euclid's algorithm finds positive integers e and f such that $de - \phi(n)f = 1$. The number d is kept private, but the number e is made public.

III. We work through a numerical example using small prime numbers.

A. Say $p = 71$ and $q = 79$, so that $n = pq = 5609$ and $\phi(n) = (p - 1)(q - 1) = 70 \times 78 = 5460$. We chose $d = 341$, which is relatively prime to 5460.

B. Euclid's algorithm verifies that $(5460, 341) = 1$ and finds the integer combination $341(1361) - 5460(85) = 1$, so $e = 1361$.

C. To send the message "Hi," we let $M = 0809$. We send $C = M^e \pmod{n} = (809)^{1361} \bmod 5609 = 4394$.

D. The bank deciphers our message by computing $(4394)^{341} \bmod 5609$, which equals 809, which the bank converts to the plaintext "Hi."

E. If both the bank and the customer have their own public key numbers, then the customer has a way of providing digital signatures so that the bank can trust that the message came from the customer. With digital signatures, not only was the customer the only one who could send the message, but the signature is also message specific, so it cannot be forged or attached to a different message.

Suggested Reading:

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 43, 45.

Silverman, *A Friendly Introduction to Number Theory*, chap. 18.

Questions to Consider:

1. If n is a composite number, why must it have a divisor larger than 1 that is no bigger than $\sqrt{n}$?

2. In the RSA method of public key cryptography, with $p = 17$ and $q = 29$, what is the chance that a numerical message M (with $0 \le M < 493$) would not be relatively prime to $n = pq = 493$?

3. For the RSA problem with $p = 17$ and $q = 29$, suppose that the bank publishes the enciphering number $e = 303$. What secret number d does the bank use to decipher its messages?

4. Do the same problem with $p = 71$, $q = 79$, and $e = 101$.

5. Here is how digital signatures work. Suppose that the bank has public key numbers e and n (with secret number d) and that you also have public key numbers e^* and n^* (with secret number d^*). To send a "signed" message M to the bank, begin by computing $C = M^e \pmod{n}$, but then compute $C^* = C^{d^*} \pmod{n^*}$, and send the message C^* to the bank, along with an unencrypted note that this message is coming from you. How does the bank decipher your message?

Lecture Sixteen
The Birth of Graph Theory

Scope: In this lecture, we introduce the subject of graph theory, an extremely useful branch of discrete mathematics, with beautiful theorems and myriad applications. In graph theory, objects are represented by vertices (dots or points) in space, and 2 vertices are connected by an edge (or line) if the objects are related in some way. We establish the basic definitions and notation and prove some of the basic theorems. We define walks, paths, trails, and cycles and then prove the first theorem of graph theory, due to Euler.

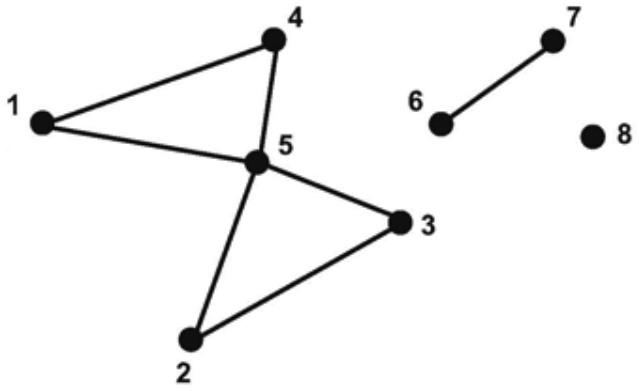
Outline

I. The first concepts of graph theory include walks, paths, trails, and cycles.

A. Although the first theorem of graph theory goes back to 1736, it is a very modern subject. Its first textbook appeared in 1958, and research journals in graph theory are less than 40 years old.

B. Although we usually think of a graph by its picture, the formal definition describes a graph in terms of sets and subsets. A graph G consists of a finite vertex set V and an edge set E consisting of size-2 subsets of V.

C. For example, the graph G pictured here



has $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and $E = \{\{1,4\}, \{1, 5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{4, 5\}, \{6, 7\}\}$.

D. A graph does not allow an edge to go from a vertex to itself (known as a loop), nor does it allow more than 1 edge to connect a pair of vertices (known as multiedges). When we want our graph to allow multiple edges, we call it a multigraph.

E. If an edge exists between x and y, then we say that x and y are adjacent. For example, in our pictured graph G, vertices 3 and 5 are adjacent.

F. The number of vertices adjacent to vertex v is called the degree of v, denoted $d(v)$. For example, $d(1) = 2$, $d(5) = 4$, and $d(8) = 0$.

G. There are various ways to "walk" along a graph.

1. A walk on a graph is a sequence of adjacent vertices where repetition is allowed. For example, $W = 1, 5, 2, 3, 5, 3, 5$ is a walk of length 6 from 1 to 5.

2. A path is a walk with no repeated vertices. For example, $P = 1, 5, 2, 3$ is a path from 1 to 3. Notice that if a walk exists from x to y, then a path exists from x to y.

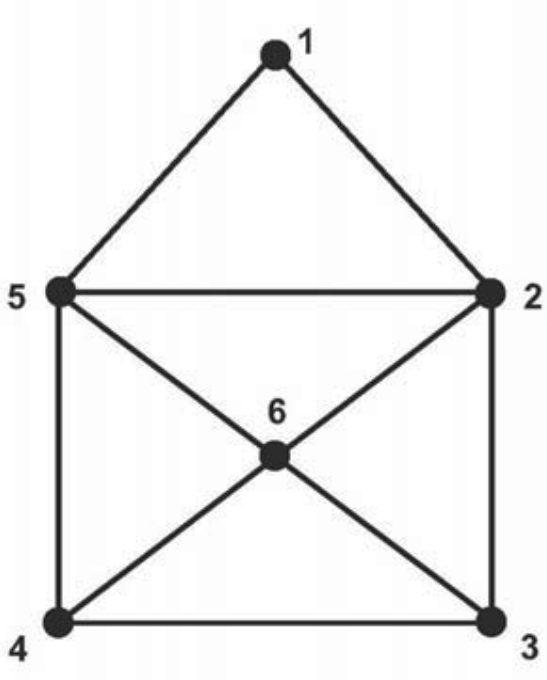
3. A trail is a walk with no repeated edges. For example, 1, 5, 2, 3, 5, 4 is a trail, and so is 1, 5, 2, 3, 5, 4. A trail is closed if it begins and ends with the same vertex.

4. A cycle (of length k) is a closed trail $v_0, v_1, \ldots, v_k$ (note that $v_k = v_0$), such that $v_0, v_1, \ldots, v_{k-1}$ is a path.

H. A graph is connected if for all vertices x and y, there is a path from x to y.

II. Leonhard Euler invented graph theory in order to solve what is the oldest theorem of graph theory.

A. Question: Can you draw this graph without lifting your pen off the paper and without retracing any edges?



B. Yes, and here's one way to do it: 3, 6, 5, 2, 6, 4, 5, 1, 2, 3, 4.

1. Such a graph is called drawable. If we remove the 2 edges at the top ({1, 2} and {1, 5}), then the graph is no longer drawable, since a trail from x to y that uses every edge must enter and exit every vertex (except x and y) an even number of times. Hence, such a graph must have at most 2 vertices of odd degree. Since this graph would have 4 vertices of odd degree, it would not be drawable.

2. Note that in the original graph, there are exactly 2 vertices of odd degree (vertices 3 and 4), so any trail that draws the graph must have endpoints 3 and 4. The altered graph cannot be drawn in such a way that it begins and ends at the same point, since that would require that every vertex have even degree.

C. We say that a graph (or multigraph) is Eulerian if it is connected and G contains a closed trail that uses every edge.

D. By our earlier argument, we see that if G is Eulerian, then G is connected and every vertex must have even degree. The converse statement is also true. The Eulerian graph theorem: If G is connected and every vertex has even degree, then G is Eulerian.

E. Eulerian graphs have applications outside of graph drawing. For example, they can be used to create de Bruijn sequences, where all 2^n binary code words of length n can be encapsulated in a single list of 2^n numbers.

F. Eulerian graphs should not be confused with Hamiltonian graphs. A graph is Hamiltonian if it contains a cycle that goes through every vertex (but might not use every edge).

Suggested Reading:

Chartrand, *Introductory Graph Theory*, chaps. 1, 3.

Hopkins and Wilson, "The Truth about Königsberg."

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 7.

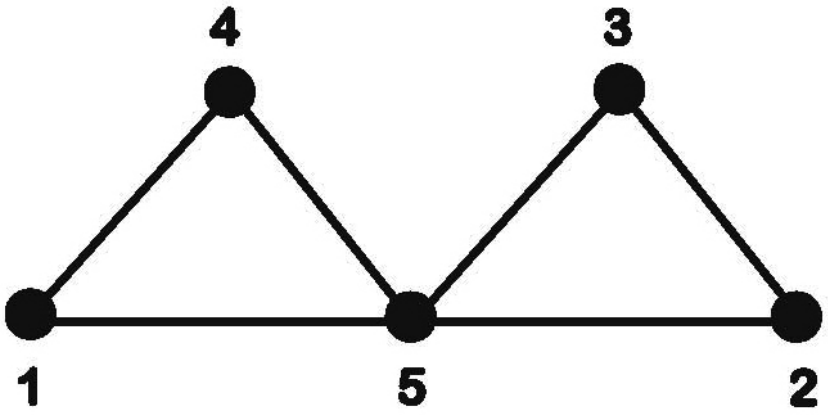
Rosen, *Discrete Mathematics and Its Applications*, chap. 8.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 46, 50.

West, *Introduction to Graph Theory*.

Questions to Consider:

1. For the graph G presented below:



a. Give the vertex set and edge set for G.

b. Find the shortest path from vertex 1 to vertex 3.

c. Is G Eulerian?

d. Is G Hamiltonian?

2. Recall that the complete graph K_n contains n vertices and that every pair of vertices is connected by an edge.

a. How many edges does the complete graph K_n have?

b. Prove that for $n \geq 3$, K_n is Eulerian if and only if n is odd.

3. Using the Eulerian graph theorem, prove that if G is a connected graph with exactly 2 vertices of odd degree, say, vertices x and y, then G can be drawn as a trail from x to y.

4. Let G_1 and G_2 be Eulerian graphs with no vertices in common. Let x be a vertex in G_1; let y be a vertex in G_2; and let G be the graph obtained by connecting G_1 and G_2 with an edge from x to y. What can you say about the new graph?

5. **a.** Draw the graph of a cube. It will have 8 vertices and 12 edges.

b. Is this graph Eulerian?

c. Is this graph Hamiltonian?

Lecture Seventeen
Ways to Walk—Matrices and Markov Chains

Scope: Given a graph, it is natural to ask how many ways you can walk from one vertex to another. To answer this question, we introduce the idea of a matrix, which is essentially a box of numbers. Matrices can be added and subtracted in a natural way, but the rule for matrix multiplication is a little unusual, and matrix division is not always possible. Any graph can be represented by an adjacency matrix, where the (i, j) entry of the matrix is 1 if vertices i and j are adjacent and is 0 otherwise. We show that if a graph has adjacency matrix A, then the number of walks from vertex i to vertex j that use exactly N steps is simply the (i, j) entry of the matrix A^N. Now suppose that when you walk on a graph, when you are at vertex i, you walk to vertex j with probability p_{ij} This is called a Markov chain. Markov chains are used for modeling random processes.

Outline

I. Considering how a computer sees a graph, we use matrices to address the question "How many ways can you walk from one vertex to another in a given graph?"

A. One way that a computer can represent a graph is by using an adjacency matrix, where the entry in the i^{th} row and j^{th} column of the matrix is the number of edges that go from i to j.

1. For example, the graph with edges $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, and $\{3, 4\}$ has the adjacency matrix that follows.

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

2. Note that this definition works for graphs, multigraphs, and oriented graphs as well.

B. Matrix addition is easy. You simply add the entries componentwise.

C. But matrix multiplication is trickier. When multiplying 2 square matrices, say $AB = C$, then C_{ij} (the entry of C in row i and column j) is the dot product of the i^{th} row of A with the j^{th} column of B. For example,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

since (1, 2) dotted with (5, 7) = 5 + 14 = 19; (1, 2) dotted with (6, 8) = 6 + 16 = 22; and so on.

D. Using adjacency matrices, we have an elegant way to count walks in a graph. Theorem: Let G be a graph (or multigraph) with adjacency matrix A. Then the number of length-L walks from vertex i to vertex j is the (i, j) entry of A^L.

II. A random walk is a walk with distinct probabilities for each step.

A. Suppose you take random steps in your graph, so that when you are at vertex i, you move to vertex j with some probability p_{ij}.

B. For the graph considered earlier, if we move to adjacent vertices with equal probability, then we have the transition probability matrix P.

$$P = \begin{bmatrix} 0 & 1/3 & 1/3 & 1/3 \\ 1/2 & 0 & 1/2 & 0 \\ 1/3 & 1/3 & 0 & 1/3 \\ 1/2 & 0 & 1/2 & 0 \end{bmatrix}$$

C. Theorem: For a random walk on graph G with transition probability matrix P, when starting at vertex i, the probability that we are in state j in L steps is the (i, j) entry of P^L.

III. The process of randomly walking on a graph is called a Markov chain. Markov chains can be used to model any process where things move randomly from one state to another.

IV. The World Wide Web can be thought of as one giant directed graph.

A. Suppose there is a directed edge from webpage i to webpage j if there is a link from page i to page j.

B. Then if we wander the Web at random, we will spend more time at webpages that are popular than at webpages that are unpopular.

C. By calculating equilibrium probabilities in a certain way, a search engine can measure a webpage's importance. This idea is exploited by many efficient search engines.

D. Similar applications of Markov chains can be found that model population dynamics, genetics, stock prices, and games like blackjack.

E. In each of these situations, your prediction of where you will be at the next moment in time is based on where you are now.

Suggested Reading:

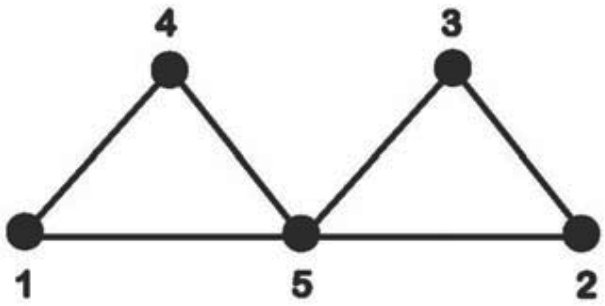
Bogart, *Introductory Combinatorics*, chap. 4.

Chartrand, *Introductory Graph Theory*, chap. 10.

Rosen, *Discrete Mathematics and Its Applications*, chap. 8.

Questions to Consider:

1. Determine the adjacency matrix for the graph below.



2. Use this adjacency matrix to determine the number of walks from vertex 1 to vertex 5 that take exactly 4 steps.

3. Draw the graph that has adjacency matrix $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

4. Suppose that a sunny day has a 50% chance of being followed by a sunny day, and a cloudy day has a 75% chance of being followed by a cloudy day.

a. Create the 2 × 2 transition probability matrix for this problem.

b. Given that today is sunny, what is the probability that it will be cloudy 2 days from now?

c. In the long run, what fraction of days are sunny?

Lecture Eighteen
Social Networks and Stable Marriages

Scope: One of the first theorems in graph theory is sometimes called the handshake theorem, which says that when a group of people meet and some of them shake hands, the total number of handshakes will always be even. In graph theoretic terms, it says that the sum of the degrees of all the vertices is equal to twice the number of edges. As an application, we extend our earlier result that among any 6 people, there must always exist 3 mutual friends or 3 mutual strangers. Building on that result and "armed" with the handshake theorem, we show that with 9 people, there must always be 3 mutual friends or 4 mutual strangers. We also discuss the stable marriage theorem, which shows that in a community with n men and n women who wish to be paired up for matrimony, there is always a way to do this in such a way that no extramarital affairs will take place.

Outline

I. Since a graph is a collection of vertices and edges, where the vertices are connected by an edge if they are related in some way, then it is not surprising that graph theory has been used to model social activities.

A. The handshake theorem says that the sum of the degrees of the vertices of a graph must be twice the number of edges.

B. The proof is that if we count the edges that leave each vertex, then every edge is counted exactly twice.

C. The following set of graphs will play an important role: A complete graph K_n consists of n vertices, where every pair of vertices is adjacent. For example, K_3 looks like a triangle and K_4 would look like a square with both diagonals included.

II. Complete graphs give us insight into the number of mutual friends and strangers using Ramsey's theorem.

A. Ramsey's (3, 3) theorem says that among any 6 people, there must exist 3 mutual friends or 3 mutual strangers. This was stated and proved in Lecture One. But we can say it another way in terms of complete graphs. If every edge of K_6 is colored red (friend) or blue (stranger), then there must exist a red K_3 or a blue K_3.

B. Ramsey's (3, 4) theorem says that any group of 10 people must contain 3 mutual friends or 4 mutual strangers. Equivalently, if every edge of K_{10} is colored red or blue, then it must have a red K_3 or a blue K_4.

C. In fact, Ramsey's (3, 4) theorem can be strengthened to 9 people: If every edge of K_9 is colored red or blue, then it must have a red K_3 or a blue K_4.

III. The stable marriage problem is another classic application of discrete mathematics to social networks.

A. Suppose that you have been hired to be the matchmaker for a town with n men and n women who wish to be paired up with each other in a logical way. Each man provides you with a list of the names of all n women, ranked from first choice to last choice, and the women similarly provide you with a list ranking all n men.

B. Your job is to provide a way to pair up the n men and n women in such a way that no extramarital affairs will take place. In other words, there is no man i and no woman j so that i and j prefer each other over the mates they have been assigned.

C. The stable marriage theorem says that your job can always be accomplished, no matter how the men and women have ranked each other. Better still, it provides an algorithm that accomplishes your task.

D. In round 1, every man proposes to his first choice. Those women who receive offers tentatively accept the best offer and tell the other men not to come back. The rejected men then propose to their next choice, and the women again tentatively accept the best offer they have so far received and tell the other proposers to go away. This process continues until eventually every woman has tentatively accepted someone (at which point there are no rejected men), and the matchmaker assigns the men to the women in this way.

E. This assignment is guaranteed to be stable. Why? Suppose man i is more interested in woman j than the woman he was assigned. But then he would have already proposed to woman j, and she rejected him for someone else, whom she preferred. Therefore, although man i is interested in woman j, woman j is not interested in man i.

F. A version of this algorithm is actually used to match medical residents with hospitals.

IV. Mathematicians have playfully created a collaboration graph in honor of Paul Erdös, who wrote more than 1400 mathematical papers (more than any other mathematician) and had more than 500 collaborators.

A. A person's Erdös number is the number of steps that it takes to get to the vertex represented by Erdös.

B. Erdös himself has an Erdös number of 0. Anyone who has written a paper with Erdös has an Erdös number of 1.

C. Anyone who has written a paper with someone who has written a paper with Erdös has Erdös number 2, and so on.

Suggested Reading:

Chartrand, *Introductory Graph Theory*, secs. 5, 8.

Rosen, *Discrete Mathematics and Its Applications*, chap. 4.

West, *Introduction to Graph Theory*, chap. 8.

Questions to Consider:

1. Find a graph with vertex set $V = \{1, 2, 3, 4, 5\}$ and the given degree sequence, or explain why such a graph cannot exist.

a. $d(1) = 1$, $d(2) = 1$, $d(3) = 2$, $d(4) = 2$, $d(5) = 2$.

b. $d(1) = 2$, $d(2) = 2$, $d(3) = 2$, $d(4) = 2$, $d(5) = 4$.

c. $d(1) = 0$, $d(2) = 1$, $d(3) = 2$, $d(4) = 3$, $d(5) = 4$.

d. $d(1) = 0$, $d(2) = 1$, $d(3) = 2$, $d(4) = 3$, $d(5) = 3$.

2. Prove that among 18 people, there must be 4 mutual friends or 4 mutual strangers. (Hint: You may use the fact that with 9 people, there must be 4 mutual friends or 3 mutual strangers.)

3. In the stable marriage problem with n men and n women, how many different lists could the matchmaker receive? (Hint: When $n = 1$, 2, and 3, the answers are 1, 4, and 36, respectively.)

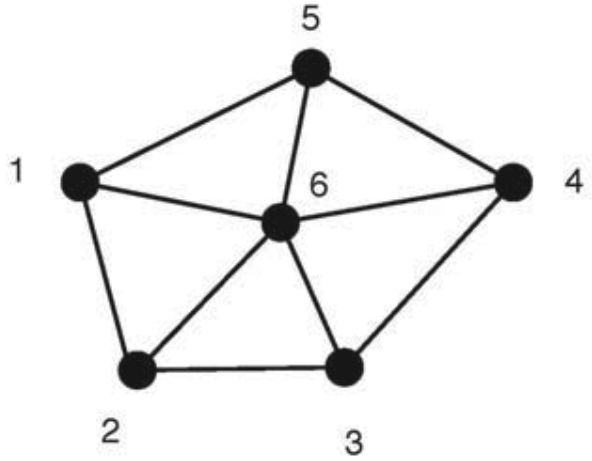
4. Suppose the matchmaker receives the following lists:

Man 1: (3, 1, 4, 2, 5; i.e., his first choice is woman 3, followed by woman 1, and so on); man 2: (1, 3, 5, 2, 4); man 3: (5, 4, 3, 2, 1); man 4: (1, 5, 4, 2, 3); man 5: (3, 4, 5, 1, 2); woman 1: (3, 5, 1, 4, 2); woman 2: (3, 1, 2, 4, 5); woman 3: (1, 2, 3, 4, 5); woman 4: (5, 3, 1, 2, 4); woman 5: (5, 4, 2, 3, 1).

a. Use the stable marriage algorithm to find a stable pairing.

b. Find another stable pairing obtained by having the women propose to the men.

5. **a.** How many perfect matchings are in the wheel graph W_6 below, consisting of 6 vertices—a cycle of 5 vertices, along with a sixth vertex that is adjacent to everything on the cycle?



b. How many perfect matchings are in the wheel graph W_n?

Lecture Nineteen
Tournaments and King Chickens

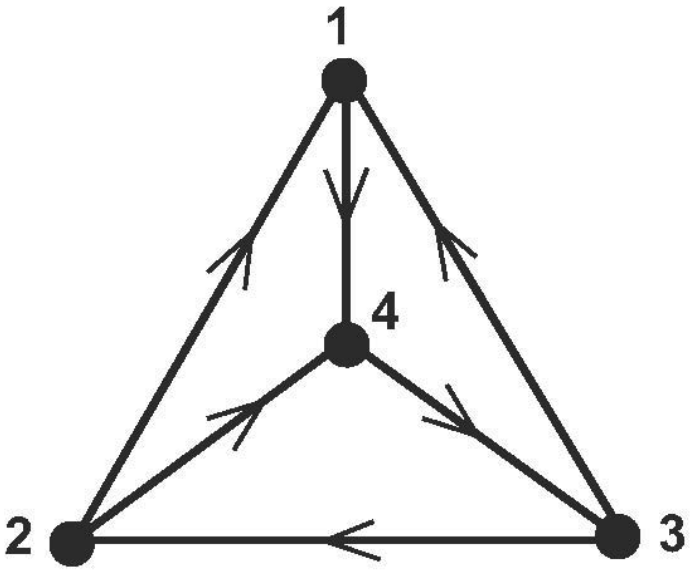
Scope: In a tournament with n people, everyone plays everyone else in a game where no ties are possible, and the winner of the match is indicated on a graph. We create a tournament graph where each player is represented by a vertex, and if player x beats player y in the tournament, then an edge is drawn as an arrow pointing from x to y. Using tournament graphs, we prove that no matter who beats whom in the tournament, we will be able to list all the players in some order $v_1, v_2, \ldots, v_n$ so that v_1 beat v_2, v_2 beat v_3, … , and v_{n-1} beat v_n. We also prove that the tournament will always contain a "king chicken": player x with the property that for any opponent y, either x beat y or there is some player z for which x beat z and z beat y.

Outline

I. We can use directed graphs to understand tournaments and the Hamiltonian path theorem.

A. A tournament is a complete graph where every edge has an orientation. An edge that points from i to j can be thought of as player i defeating player j in a tournament where everyone plays everyone else in 1 game.

B. For example, here is a tournament with 4 players.



C. Notice that in this tournament, we have 1 → 4→ 3→ 2. This is called a (directed) Hamiltonian path because it is a path that goes through every vertex of the tournament.

D. Hamiltonian path theorem: Every tournament has a Hamiltonian path. That is, for $n \geq 1$, for any tournament on n vertices, there is always a sequence of vertices $v_1, v_2, \ldots, v_n$ such that $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \ldots \rightarrow v_n$.

II. Professor Steve Maurer of Swarthmore College developed the king chicken theorem to explain the pecking orders of chickens.

A. Definition: In a tournament, x is a king chicken (or king) if for every opponent y, either $x \rightarrow y$ or there exists a player z such that $x \rightarrow z \rightarrow y$. In other words, a king is a player that can walk to any vertex in at most 2 steps.

B. The king chicken theorem: Every tournament has at least 1 king chicken.

C. Proof: Let v be a vertex with the maximum outdegree (most victories). Suppose v has k victories and v beat $v_1, v_2, \ldots, v_k$. We claim that v must be a king, since otherwise there would exist another vertex u such that $u \rightarrow v$ and $u \rightarrow v_1, \ldots, v_k$. But then u beat at least $k + 1$ opponents, contradicting the assumption that v had the most victories.

D. Theorem: If a player loses, then it must lose to a king.

1. Proof: Let v be any vertex that has at least 1 loss. Let W be the set of vertices that beat v, and let L be the set of vertices that lost to v. If we just focus on the tournament consisting of the players in W, then by the king chicken theorem, it contains a king (of the set W). Call that king k.

2. We claim that k is a king of the entire tournament, since k can reach v in 1 step and can reach any vertex in L in at most 2 steps by way of v. Hence v loses to k, a king.

E. A vertex v is an emperor if $v \rightarrow w$ for all w. Clearly, if v is an emperor, then it is also a king. Conversely, if a tournament has exactly 1 king, then that king must also be an emperor.

F. Corollary: No tournament has exactly 2 kings. Proof: Suppose the tournament has 2 kings, a and b, and say that $a \rightarrow b$. Now a had to lose to someone (else he could not be a king). But then a had to lose to a king, and therefore the tournament has at least 1 more king.

III. The preceding theorems suggest many natural questions and extensions.

A. For example, in a tournament with n players, is it possible for every player to be a king? We have seen that the answer is no when $n = 2$. It is also impossible when $n = 4$. But surprisingly, it is possible for all other values of n.

B. Moreover, we can build on these results to prove that for $1 \leq k \leq n$, unless $k = 2$ or $n = k = 4$, it is possible to create a tournament with n players that has exactly k kings.

Suggested Reading:

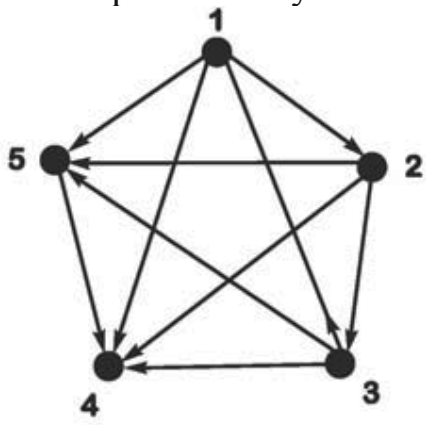
Chartrand, *Introductory Graph Theory*, sec. 7.

Maurer, "The King Chicken Theorems."

West, *Introduction to Graph Theory*, chap. 1.

Questions to Consider:

1. Consider the tournament represented by the oriented graph below.



a. Does the tournament have an emperor?

b. Find a directed Hamiltonian path.

c. Which players are king chickens?

2. How many possible tournaments on n vertices exist?

3. For an oriented graph, let $d(x, y)$ be the shortest number of steps to go from x to y, where every step is along an edge in the oriented direction.

a. In the oriented graph shown in question 1 above, compute $d(3, 2)$.

b. Prove that in any tournament, for any vertices x and y, $d(x, y) \neq d(y, x)$.

4. In our lecture, we saw that in a tournament, it was possible with 5 players for each player to be tied for first place (i.e., having the most victories). Prove that this is impossible to do with 6 players. Is it ever possible with an even number of players?

Lecture Twenty
Weighted Graphs and Minimum Spanning Trees

Scope: Next we "branch off" to describe a special kind of graph that arises in many applications of graph theory. A tree is a connected graph with no cycles. (An unconnected graph with no cycles is called a forest.) Trees have a very simple structure that makes them useful for data storage and communication. For example, one can prove that every tree with n vertices always has exactly $n - 1$ edges. Likewise, every tree must contain at least 1 leaf, a vertex with just 1 neighbor. Finally, it can be shown that in a tree, every pair of vertices is connected by a unique path. We apply these theorems to solve the minimum spanning tree problem, showing how the cheapest connected substructure of a weighted graph can be determined by a greedy algorithm.

Outline

I. A tree is a connected graph with no cycles.

A. A disconnected graph without cycles is called a forest, and its connected components are trees.

B. How many trees are there with vertices labeled 1 through n?

1. Clarification: 2 trees are equal if they have the same set of edges. Thus a tree like 1-2-3 is the same as the tree 3-2-1.

2. Cayley's formula says that for $n \geq 1$, the number of trees with n vertices is n^{n-2}.

C. In a tree, a vertex of degree 1 is called a leaf.

D. Theorem: Every tree T with at least 2 vertices has at least 1 leaf.

E. Note that when a leaf (and its 1 edge) are removed from a tree, the resulting graph is still a tree. This is useful for many induction proofs about trees.

F. Theorem: Every tree with n vertices has exactly $n - 1$ edges.

II. Trees are often used as efficient data structures where information is stored at the vertices.

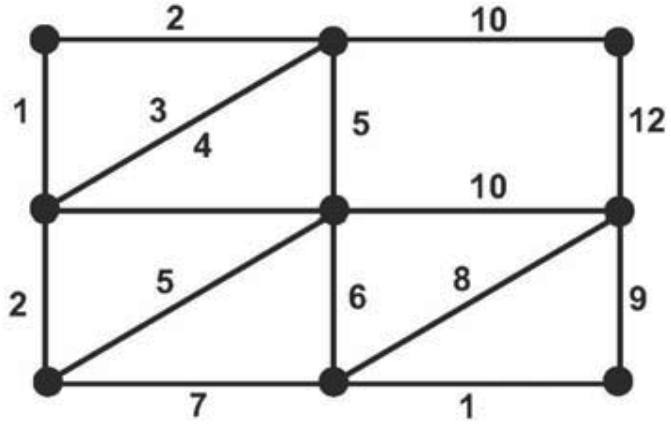
A. For example, when you call someone on your cell phone, your number is picked up by a tower that communicates your number to another tower, and another, until it reaches the top of a tree (called the root) and then finds the person you are trying to reach, who is another leaf of the tree.

B. Trees make excellent data structures for storing words in a dictionary. With about 2^n data points, a search of a binary tree takes only about n steps, compared to about 2^{n-1} steps to search a simple list!

C. The following theorem is useful for communicating between vertices. Theorem: If T is a tree, then any 2 vertices are connected by a unique path.

III. A minimum spanning tree is a tree that connects all the vertices while minimizing the sum of the weights of the edges.

A. Consider a weighted graph like G, the one shown here.

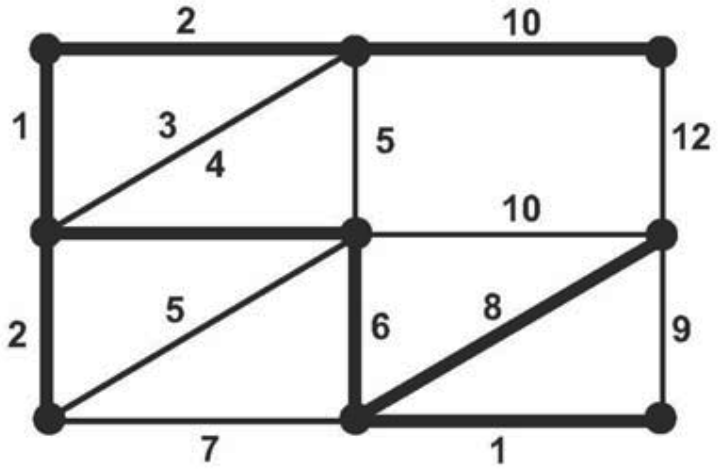


B. This could be a network of roads or computers, and the weight of an edge could represent the cost of traveling from 1 city to another, paving a road between houses, or getting 2 computers to communicate. The problem is to find a spanning tree (a tree that connects all the vertices of G) that minimizes the sum of the weights of the edges.

IV. This problem can be solved using the following greedy algorithm.

A. Choose 8 edges, 1 at a time, from smallest cost to largest cost, where we ignore an edge only if its inclusion would create a cycle.

B. Following this algorithm on the above graph results in the following spanning tree of weight 34.



C. Theorem: A tree produced by the greedy algorithm is guaranteed to be a minimum spanning tree.

V. Suppose we wish to know how many spanning trees a graph G has.

A. The answer depends on the adjacency matrix of G and the determinant.

1. The determinant of a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $ad - bc$.

2. The determinant of a 3×3 matrix $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ is $aei + bfg + cdh - (gec + hfa + idb)$.

3. The formula for the $n \times n$ determinant is the sum of $n!/2$ products minus the sum of $n!/2$ other products—although for $n > 3$, there are quicker ways to compute the determinant without using its formula.

B. The number of spanning trees in a graph is just the determinant of a particular matrix obtained by subtracting the adjacency matrix A from the diagonal matrix D.

1. Let D be the diagonal matrix where the i^{th} number on the diagonal is the degree of vertex i and everything else is 0.

2. Because every row sums to 0, it turns out that the determinant of $D - A$ would always be 0. But if we remove any row and its corresponding column from matrix $D - A$, the determinant of that smaller matrix is equal to the number of spanning trees of G!

VI. The good news about trees is that they are very efficient. The bad news is that they are very vulnerable. If any of your edges breaks, the graph becomes disconnected. Thus, when designing a network, it is generally a good idea to build in some redundancy.

Suggested Reading:

Chartrand, *Introductory Graph Theory*, sec. 4.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chaps. 8–9.

Rosen, *Discrete Mathematics and Its Applications*, chap. 9.

West, *Introduction to Graph Theory*, chap. 2.

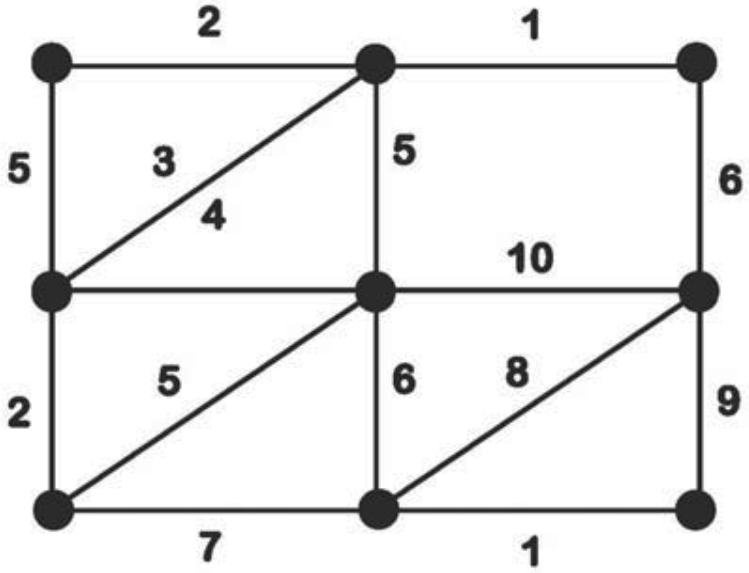
Questions to Consider:

1. There are essentially 6 different trees with 6 vertices that have fundamentally different pictures. Draw them.

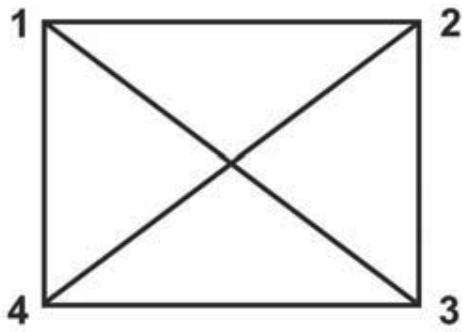
2. Count the ways to label each of the above trees to verify Cayley's formula that there are $6^4 = 1296$ trees with vertex set $\{1, 2, 3, 4, 5, 6\}$.

3. We know that in a tree, there is a unique path connecting any given pair of vertices. Prove the converse theorem: If a graph G has the property that for any pair of vertices x and y, there is a unique path from x to y, then G must be a tree.

4. Find the minimum weight spanning tree for the weighted graph below.



5. Use determinants to compute the number of spanning trees inside the complete (labeled) graph of K_4 below. Why is the answer not a surprise?



Lecture Twenty-One
Planarity—When Can a Graph Be Untangled?

Scope: Next we introduce the notion of a planar graph, which is a graph that can be drawn on a sheet of paper in such a way that none of its edges cross, and we prove (another!) theorem due to Euler that says that if a connected planar graph has n vertices, e edges, and f faces, then $n - e + f = 2$. The same formula applies to the vertices, edges, and faces of polyhedra. As a consequence, we show that a planar graph with n vertices has at most $3n - 6$ edges. This leads us to discover 2 graphs that cannot be straightened out, which are an essential part of all nonplanar graphs.

Outline

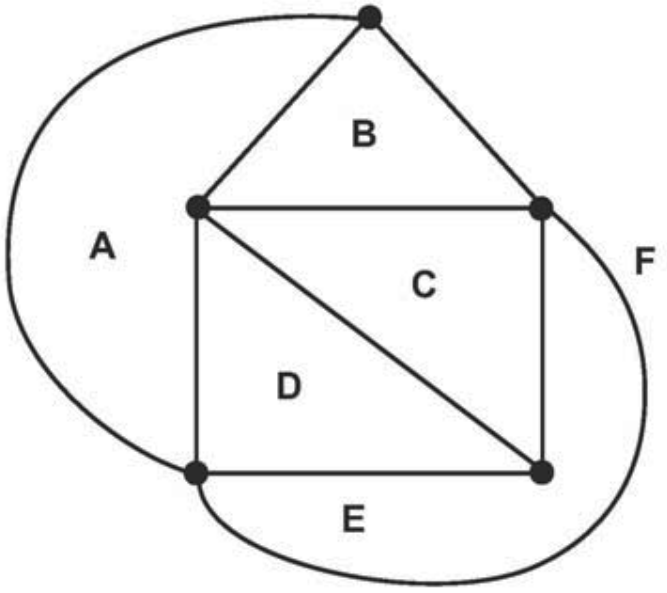
I. Some graphs are more useful when they can be drawn without crossing edges (e.g., graphs of circuit boards or highway systems).

A. Definition: A planar graph is a graph that can be drawn in such a way that no edges cross.

1. For example, all trees are planar graphs.

2. K_4 is planar since it can be drawn as a triangle with a vertex inside it, with none of the 6 edges crossing.

B. Every planar graph divides the plane into regions or faces, including the external face. For example, this graph has 6 faces.



II. Euler's planar graph theorem: If G is a connected plane graph with n vertices, e edges, and f faces, then $n - e + f = 2$. For example, the graph above has $n - e + f = 5 - 9 + 6 = 2$.

A. Euler's theorem also applies to 3-dimensional objects (called polyhedra) like the cube, which has 8 vertices, 12 edges, and 6 faces. Notice that $n - e + f = 8 - 12 + 6 = 2$.

B. Euler's theorem can also be used to show that it is impossible to construct Venn diagrams with 4 (or more) circles.

III. Our next theorem proves that planar graphs cannot have too many edges.

A. Theorem: If G is a planar graph with $n \geq 3$ vertices and e edges, then $e \leq 3n - 6$.

B. The theorem fails when $n = 1$ or 2 since K_1 and K_2 have $e > 3n - 6$.

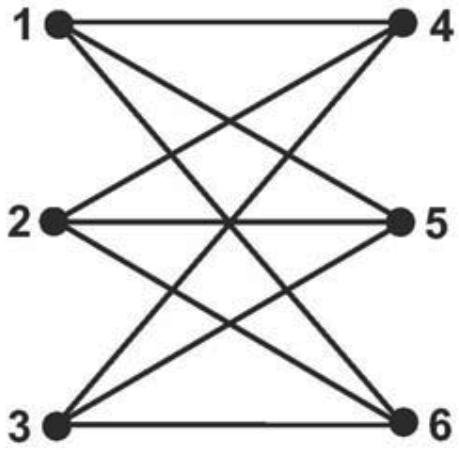
C. For the proof of this theorem, we consider 2 cases: Either G is connected or G is not connected.

D. Notice that $e = 3n - 6$ is achievable, for example, on the graphs K_3 ($n = 3$, $e = 3$) and K_4 ($n = 4$, $e = 6$).

E. Corollary: K_5 is nonplanar. The proof is simple. K_5 has $n = 5$ vertices and $e = 10$ edges. Since $e > 3n - 6 = 9$, K_5 cannot be planar.

IV. The converse statement—if $e \leq 3n - 6$, then G is nonplanar—is false.

A. For example, the complete bipartite graph $K_{3,3}$ (pictured below) has $n = 6$ vertices and $e = 9 < 12 = 3n - 6$ edges. Nevertheless, $K_{3,3}$ is nonplanar.



B. In fact, K_5 and $K_{3,3,}$ are the simplest nonplanar graphs in that every nonplanar graph must contain 1 of them.

C. Specifically, Kuratowski's theorem says that every nonplanar graph contains inside it K_5 or $K_{3,3}$ or a subdivision of K_5 or $K_{3,3.}$ A subdivision of a graph is the same graph with some new vertices of degree 2 added to some of the edges of G.

Suggested Reading:

Chartrand, *Introductory Graph Theory*, sec. 9.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 12.

Rosen, *Discrete Mathematics and Its Applications*, chap. 8.

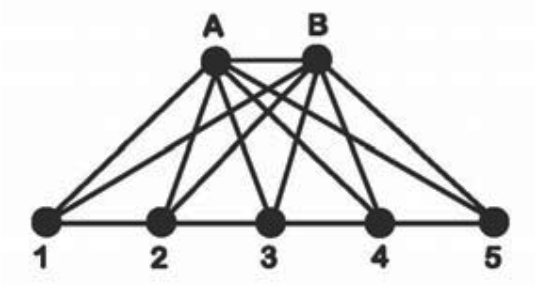
Scheinerman, *Mathematics: A Discrete Introduction*, sec. 52.

West, *Introduction to Graph Theory*, chap. 6.

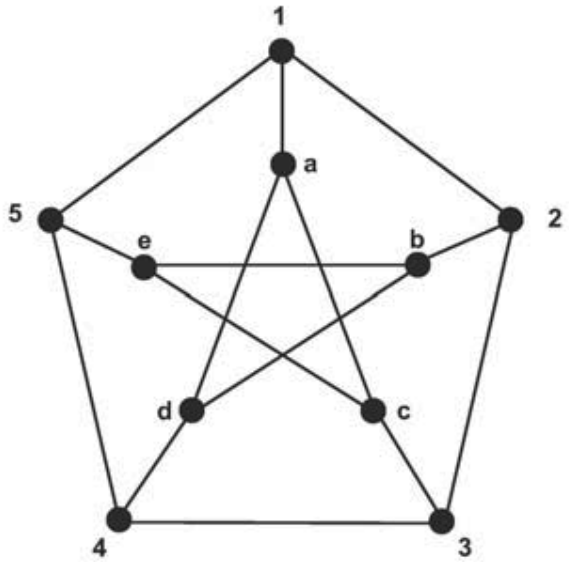
Questions to Consider:

1. If G is a planar graph with 9 vertices and 15 edges, how many faces must it have?

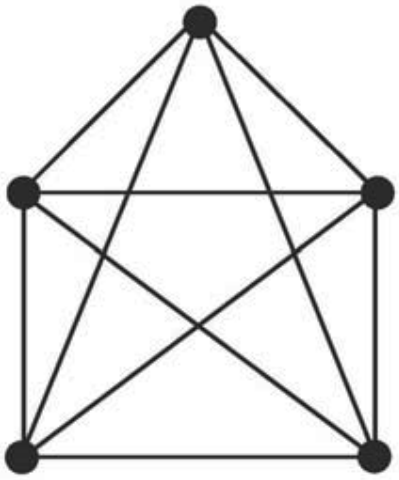
2. Show that the graph below is planar.



3. In the graph below (sometimes called the Petersen graph), every cycle has length at least 5. Use this fact and Euler's planar graph theorem to prove that it is nonplanar.



4. Another way to prove that the Petersen graph is nonplanar is to find a subdivision of K_5 (below) or $K_{3,3}$ (shown in section IV of the outline above) inside it. Why could it not have a subdivision of K_5 in it? Find a subdivision of $K_{3,3}$ in it.



Lecture Twenty-Two
Coloring Graphs and Maps

Scope: One of the most famous problems from graph theory is the 4-color theorem, which says that a map of states can always be colored in such in a way that no adjacent states are assigned the same color and that we need at most 4 colors to achieve this. This problem was unsolved for centuries and has only been proved recently with considerable computer assistance. After showing which graphs can be colored using at most 2 colors, and how any map can be converted to a planar graph, we present the essential theorems of planar graph coloring. Next we provide a brilliant proof of the 5-color theorem, followed by a flawed proof of the 4-color theorem. It took experts 10 years to detect the flaw, then nearly 100 years to finally prove the theorem true.

Outline

I. Planar graphs play an important role in proper colorings of graphs and maps.

A. Given a graph G, a coloring of G is obtained by assigning a color to every vertex (repetition of colors allowed). It is called a proper coloring if no adjacent vertices have the same color.

B. We say that a graph is k colorable if it can be properly colored using at most k colors. The smallest number k for which a graph G is k colorable is called the chromatic number of G. For example, the complete graph K_n has chromatic number n, since every vertex must be given a different color.

C. A closely related idea is proper map coloring, where every state is assigned a color so that no states that share a common border are given the same color. (We assume that states are connected regions and that adjacent states need to have more than a point in common; they must share a common boundary.)

D. The 4-color theorem says that every map can be properly colored using at most 4 colors. It was one of the most famous unsolved problems in mathematics until a few decades ago, and its final proof was controversial. Its proof took hundreds of pages, so we will not prove it here, but we will prove the 5-color theorem.

E. We can represent any map-coloring problem as a vertex-coloring problem by creating the dual graph of the given map: We insert a vertex at the capital of each state and connect 2 capitals with an edge if they share a common border. A proper coloring of the original map corresponds to a proper coloring of the dual graph, which is always planar.

F. Thus to prove the 5-color theorem for maps, it suffices to prove the 5-color theorem for coloring the vertices of a planar graph.

II. Before we prove the 5-color theorem, we establish the following lemma (or theorem): Every planar graph G must contain a vertex of degree ≤ 5.

III. The 6-color theorem: For any planar graph G, the vertices of G can be properly colored with at most 6 colors.

A. Proof (by induction on n, the number of vertices): Base case. The theorem is clearly true when G has at most 6 vertices.

B. By the induction hypothesis (IHOP): Assume the theorem is true for planar graphs with k vertices. Our goal is to prove it for planar graphs with $k + 1$ vertices.

C. Let G be a planar graph with $k + 1$ vertices. By our lemma, there is a vertex v with degree at most 5. Temporarily remove v (and its edges) from G to produce graph $G - v$.

D. Since $G - v$ is still planar and has k vertices, then by IHOP, we can properly color $G - v$ with at most 6 colors.

E. Bringing v back to the graph, since it has degree at most 5 and we have 6 colors at our disposal, we can assign v a color that is different from its neighbors. Hence G is 6 colorable.

IV. The 5-color theorem: For any planar graph G, the vertices of G can be properly colored with at most 5 colors.

A. The beginning of the proof is virtually the same as the beginning of the proof of the 6-color theorem. (See outline points A through D above, replacing the number 6 with the number 5.)

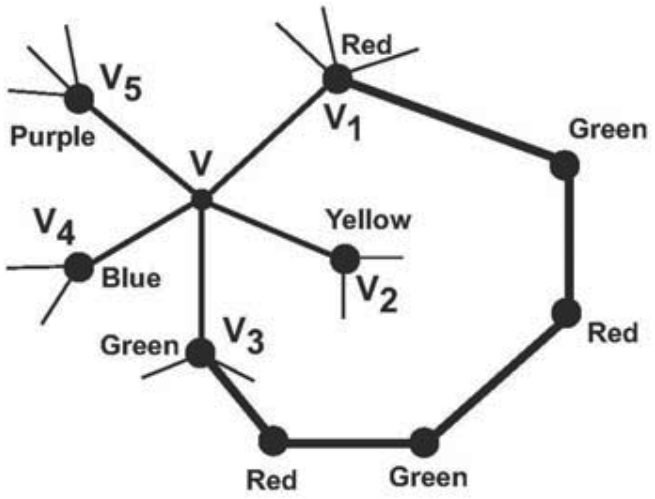
B. Bringing v back to the graph, if the number of colors used by the neighbors of v is less than 5, then with 5 colors at our disposal, we can assign v a color that is different from its neighbors, which would show that G is 5 colorable.

C. Hence it remains to consider the case where v has 5 neighbors, but none of them were assigned the same color in the proper coloring of $G - v$. We call its neighbors $v_1, v_2, \ldots, v_5$ (listed clockwise around v) and suppose that in the proper coloring of $G - v$, they were given the colors red, yellow, green, blue, and purple, respectively.

D. Now suppose we temporarily ignore all edges of G, except for the ones connecting red vertices with green vertices.

1. If vertices v_1 and v_3 are in different connected components, then in the connected component containing v_1, we can swap the colors red and green and then bring back all the edges of G so that $G - v$ is still properly colored. But now v_1 and v_3 are both green. Thus we can assign v the color red, and we have properly colored G using at most 5 colors.

2. If vertices v_1 and v_3 are in the same connected component, then there is a fence that surrounds v_2 using v, v_1, v_3, and possibly other red and green vertices, as pictured below.



E. Since v_2 is surrounded by a red-green fence and G is planar, there is no way for v_4 to reach v_2 by a blue-yellow path. Thus we can interchange the colors of blue and yellow on the connected component of G containing v_4 that uses only edges that connect blue and yellow vertices. Here, v_4 and v_2 will both be yellow, so we can assign v the color blue, and we have properly colored G with at most 5 colors.

V. The 4-color theorem.

A. Although the 4-color problem was introduced to the mathematics community in 1852, it remained an open question until it was proved in 1977 by Wolfgang Haken and Kenneth Appel.

B. Their proof required the construction of a set of over 1000 different graphs, with a computer program checking the logic for each of these cases.

VI. The 4-color theorem can be generalized to other surfaces, such as globes or donuts.

VII. How many different ways can you properly color a graph?

A. For any graph with n vertices, the number of proper colorings using at most k colors is an n^{th}-degree polynomial with variable k called the chromatic polynomial of G.

B. The leading coefficient is always 1, and the next term is the negative of the number of edges in G.

C. The chromatic number is the smallest positive integer z for which $f(z) > 0$, and $f(-1)$ tells you the number of ways you can orient the edges so there are no directed cycles.

D. A greedy algorithm can tell whether a graph is 2 colorable—also known as bipartite—but a $1 million prize awaits whoever can discover an efficient algorithm for determining whether any given planar graph is 3 colorable.

Suggested Reading:

Chartrand, *Introductory Graph Theory*, sec. 9.

Lovász, Pelikán, and Vesztergombi, *Discrete Mathematics*, chap. 13.

Rosen, *Discrete Mathematics and Its Applications*, chap. 8.

Scheinerman, *Mathematics: A Discrete Introduction*, secs. 51–52.

West, *Introduction to Graph Theory*, chaps. 5–6.

Wilson, *Four Colors Suffice*.

Questions to Consider:

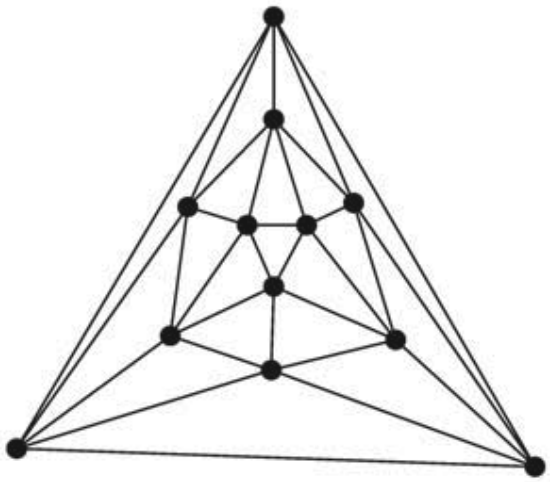
1. Explain why the complete graph K_n has chromatic number n. If we remove a single edge from K_n, will it have chromatic number $n - 1$?

2. Prove that every tree with $n \geq 2$ vertices has a chromatic number of 2. (Hint: Use a proof by induction on the number of vertices.)

3. Suppose you have m colors at your disposal. Show that the number of ways to properly color a tree with $n \geq 1$ vertices is $m(m-1)^{n-1}$. (Again, try a proof by induction.)

4. We showed that every planar graph has at least 1 vertex of degree 5 or less. Why must, in fact, every planar graph with at least 2 vertices contain at least 2 vertices with degree 5 or less?

5. The planar graph shown below has an interesting property. Can you see what it is? It is a counterexample to a statement that, if it had been true, would have led to a much simpler proof of the 5-color theorem (and the 4-color theorem).



6. A math department plans to offer 7 discrete math courses next semester, namely: Abstract Algebra (A), Combinatorics (C), Data Structures (D), Graph Theory (G), Number Theory (N), Probability (P), and Statistics (S). The math majors and the courses they plan to take are as follows.

Archimedes: A, C, D

Bézout: C, G, S

Carmichael: G, N

Dijkstra: C, D

Euler: D, N

Fermat: C, G

Gauss: N, P

Hardy: G, D

Isaac: A, C

Jacoby: A, C, S

Kuratowski: P, S

Lucas: A, P

How many time periods are needed for these 7 courses? (Hint: This is a graph-coloring problem in disguise.)

Lecture Twenty-Three
Shortest Paths and Algorithm Complexity

Scope: In this lecture, we describe and analyze Dijkstra's algorithm for solving the shortest path problem. An algorithm is a systematic method for solving a problem, and we say that this algorithm is efficient because the time required to solve such a problem is at most a polynomial function of n, where n is the number of vertices. By contrast, other problems are not known to have an efficient solution. This leads to a discussion of the complexity classes P and NP as well as the most famous unsolved problem in theoretical computer science, with a $1 million bounty on its head.

Outline

I. The shortest path problem can be solved efficiently using Dijkstra's algorithm.

A. Given a graph where every edge has a nonnegative weight, we seek to find the shortest path from some vertex A to another vertex B.

B. We will solve this using Dijkstra's algorithm, which will find the shortest path from A to all vertices in G. (We shall refer to vertices as "nodes" for this algorithm.) The weight of the edge connecting nodes x and y is $w_{xy} \geq 0$. At the end of the algorithm, we will know $C(x)$, the cost of the shortest path from A to x, along with the parent node of x on the shortest path from A to x.

C. Dijkstra's algorithm.

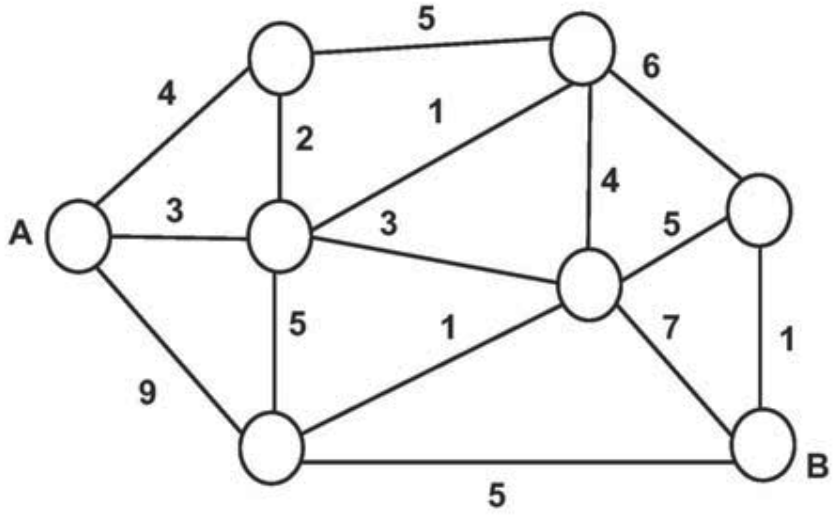
1. Step 0. Temporarily assign $C(A) = 0$ and $C(x) = \infty$ for all other x's.

2. Step 1. Find the node with the smallest temporary value of $C(x)$. (If there are no temporary nodes or if $C(x) = \infty$, then stop.) Node x is now labeled as permanent.

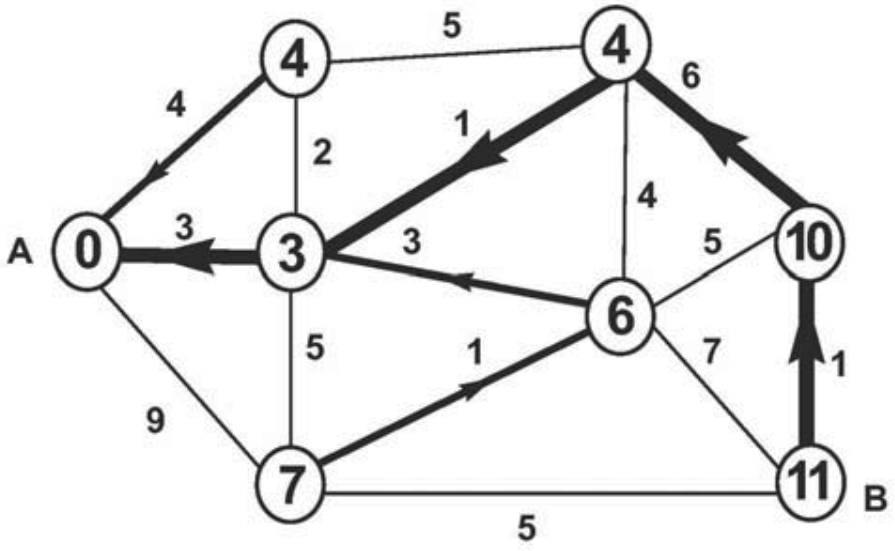
3. Step 2. For each temporarily labeled node that is adjacent to x, make the following comparison: If $C(x) + w_{xy} < C(y)$, then $C(y)$ is changed to $C(x) + w_{xy}$, and y is assigned to have parent x.

4. Step 3. Return to step 1.

D. For example, suppose Dijkstra's algorithm is given a graph like this.



E. At the conclusion of the algorithm, the graph will look like this, where the number written inside of node x is $C(x)$. The bold edges form a tree of shortest paths and connect each edge to its parent node. To find the shortest path from A to x, simply follow the unique bold path from A to x. The shortest path from A to B has total cost 11.



II. A whole class of problems has efficient algorithms.

A. Given a problem of size n, an algorithm with run time $O(n^k)$ for some k is called a polynomial-time algorithm. These algorithms are efficient.

B. The computational complexity of a problem is the run time of the fastest algorithm for solving that problem.

C. We look at some problems that have efficient algorithms.

III. For many other problems, no efficient algorithm is known.

A. For example, if G has n vertices, then to determine if it is 3 colorable, we could try all possible colorings, but the time to do that is $O(3^n)$, which is not polynomial. Likewise, the Hamiltonian path problem can be done in time $O(n!)$, but that is even worse. These algorithms are called exponential time algorithms.

B. In fact, if we could find an efficient algorithm to solve any one of these hard problems, it could be turned into an efficient algorithm to solve thousands of other hard problems.

IV. Computer scientists have defined 2 complexity classes, called P and NP. The complexity class P is the set of decision problems that can be solved in polynomial time. (A decision problem is a problem with a yes or no answer.) Some examples include: Is G Eulerian? Is G 2 colorable? Does G have a path from A to B with cost below 100?

A. The complexity class NP is the set of decision problems where a yes answer can be verified in polynomial time. NP stands for nondeterministic polynomial.

1. NP includes all problems in P, like the ones listed above.

2. NP also includes "harder" problems: Does G have a Hamiltonian path? Is G 3 colorable? Is there a Hamiltonian cycle with total cost below 100? These are examples of NP-complete problems, where it has been shown that if any of these problems has a polynomial time solution, then every problem in NP would have a polynomial time solution. This would imply that P = NP.

B. Does P = NP? Most computer scientists do not think so, but nobody has been able to prove it (or find an efficient algorithm for any of the NP-complete problems). The Clay Mathematical Institute has offered a $1 million prize for anyone who discovers and publishes such a proof or algorithm.

Suggested Reading:

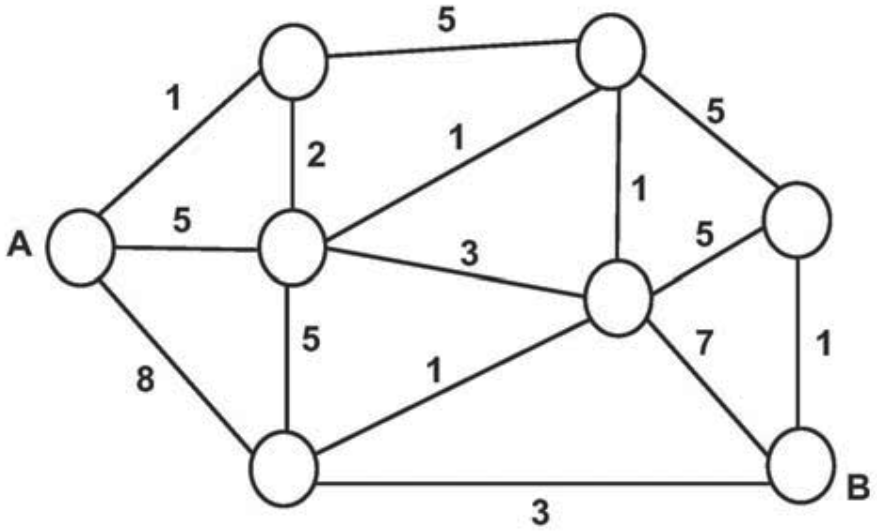
Garey and Johnson, *Computers and Intractability*.

West, *Introduction to Graph Theory*, app. B.

Wilf, *Algorithms and Complexity*.

Questions to Consider:

1. Using Dijkstra's algorithm, find a tree of shortest path from vertex *A* to all other vertices. In particular, what is the cost of the shortest path from *A* to *B*?



2. We noted how Dijkstra's algorithm can be used to determine whether a graph is connected. Suppose we have a connected graph. Provide an efficient way to determine whether it contains a cycle.

3. Which of these problems belong to the complexity class NP? (In other words, which of these problems are decision problems where a yes answer has a simple verification?)

- **a.** Does a graph contain a path that goes through at least half of the vertices?
- **b.** Does an integer n contain a divisor d where $1 < d < n$?
- **c.** Given a list of positive and negative integers, is there a subset of these integers that sums to 0?
- **d.** Given a list of positive and negative integers, do all subsets of these integers have a nonzero sum?
- **e.** Does a graph have a perfect matching (that is, it is possible to find a collection of edges in the graph so that every vertex is incident to exactly 1 edge of the collection)?
- **f.** Find the longest path in a weighted graph.

Lecture Twenty-Four
The Magic of Discrete Mathematics

Scope: We take a look back at some common themes of discrete mathematics as well as a look ahead at some topics that you can pursue to build on your solid foundation. We also include some truly magical applications of the material in this course.

Outline

I. There are numerous places where the 3 major fields of discrete mathematics (combinatorics, number theory, and graph theory) overlap.

- **A.** We saw how proofs, especially proofs by induction, played an important role in all 3 topics and how counting methods were often applied outside of the combinatorics lectures.
- **B.** We saw how the powers of 2 arise as the solution to counting problems but also provide us with additive building blocks for the integers.
- **C.** We saw Fibonacci numbers make cameo appearances in all 3 fields.
- **D.** We were introduced to many mathematicians, but the one we encountered most often was Leonhard Euler. We saw 3 theorems that were named after him: 1 in number theory, 2 in graph theory, and we will soon see 1 in combinatorics.

II. Discrete mathematics is often a prerequisite to many upper-division courses in mathematics and computer science, some of which we highlight here.

- **A.** Abstract algebra is the language of symmetry, and one of its main topics is group theory. A group is a set that has lots of structure.
- **B.** In set theory and logic, you learn how sets and logical symbols have an algebra all of their own.
- **C.** Earlier we encountered binary trees as a means of storing information. In a course on data structures and algorithms, you are exposed to other ways to store data that have nice properties.
- **D.** In a full-length course on combinatorics, you would certainly spend some time learning about generating functions.

E. In a full-length course on number theory, the prime numbers take on different personalities.

F. In a course on graph theory, you would explore more properties of graph coloring.

III. Some magic tricks are based on discrete mathematics.

A. Write down the following 3 numbers: your phone number (P), the number 8, and then $8P$. Add those numbers together. Add the digits of your answer together, resulting in a 2-digit number. Then add the digits of your 2-digit number. You will always get 8. Why? Their sum is $9P + 8$, which is congruent to 9 (mod 8).

B. If 16 cards are placed face down in a 4×4 grid with aces on the diagonal and 4 face-up cards on the spots that are diagonally adjacent to the aces, then after the cards are folded onto 1 spot, all 4 aces will be facing in the opposite direction from the rest of the cards. The secret is based on parity.

C. Using a complete set of dominoes, with 1 domino secretly removed (say the 3-4 domino), ask your volunteer to arrange the dominoes in 1 long line, with the requirement that touching dominoes have matching numbers. Then the endpoints of the domino chain are guaranteed to be 3 and 4. The secret is based on Eulerian paths, where every domino represents an edge of K_7. Every vertex has even degree except vertices 3 and 4.

IV. With magical mathematics—such as that of magicians like Euler and Ramanujan—even after seeing what they accomplished, we are still mystified as to how they did it.

V. My hope is that you now see how *discrete* mathematics can be a source of *continuous* enjoyment. At least that is what I am counting on!

Suggested Reading:

Benjamin and Brown, *Biscuits of Number Theory*.

Benjamin and Quinn, *Proofs That Really Count*.

Bogart, *Introductory Combinatorics*.

Graham, Knuth, and Patashnik, *Concrete Mathematics*.

Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*.

West, *Introduction to Graph Theory*.

Questions to Consider:

1. The Fibonacci identity given in the lecture, $\sum_{k=0}^{n}\binom{n}{k}F_k = F_{2n}$, has a nice combinatorial proof using tilings. We do this by first rewriting the identity using "little *f*" notation: $\sum_{k=0}^{n}\binom{n}{k}f_{k-1} = f_{2n-1}$. The right side counts the ways to tile a board of length $2n - 1$ with squares and dominoes. We claim that the left side does the same. To see this, note that any board of length $2n - 1$ must have at least n tiles—since if it had $n - 1$ tiles, its length would be at most $2(n - 1) = 2n - 2$. To complete the proof, show that the number of tilings with exactly k squares among the first n tiles is $\binom{n}{k}f_{k-1}$.

2. Take any 4-digit number (except for one where all the digits are the same, like 7777). Scramble the digits to create a second 4-digit number. Now subtract the smaller number from the larger. (For example, if your 4-digit number was 2358, and you scrambled them to get 5382, you would now calculate 5382 − 2358.) Now take the answer to the subtraction problem and sum the digits. If you have a 1-digit number, then stop. If you have a 2-digit number, then sum the digits to obtain a 1-digit number. What number will you always end up with, and why?

3. The domino prediction trick in the lecture used dominoes that had 2 different numbers from the set {0, 1, 2, 3, 4, 5, 6}. Would the trick have worked if the dominoes came from the set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}?

4. Place 5 cards in front of you, from left to right: ace, 2, 3, 4, 5. Place your finger on the ace or the 5, then take 5 steps. At each step, you can move your finger to the left or to the right, as long as you stay on the cards. Now remove the ace and the 5 (since your finger will not be there) and take 5 more steps. What card will you end on? Why does this trick work?

Answers to Questions to Consider

Lecture One

1. The discrete situations are a, d, e, and h.

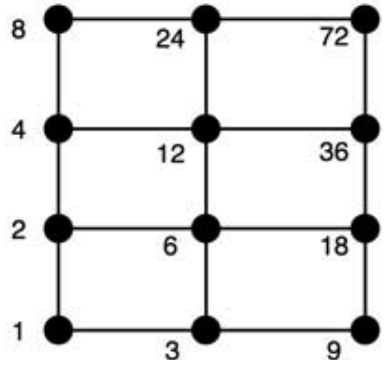
2. **a.** There are $3^3 = 27$ ternary code words of length 3.

b. There are 3^n ternary code words of length n.

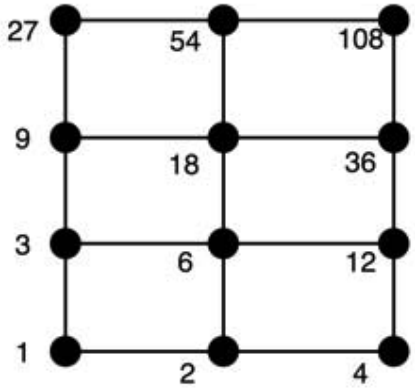
3. When doing long division of m/n, there are only n possible remainders: $0, 1, \ldots, n - 1$. When doing long division, if you ever reach a remainder of 0, the fraction terminates. Otherwise, you will eventually have a remainder that you have seen before. At this point, the fraction will repeat.

4. A fraction $1/n$ will have a terminating decimal expansion if and only if the only prime factors of n are 2 or 5. That is because a terminating decimal expansion can be written as a decimal with a denominator that is a power of 10. For example, the decimal $0.abcd$ is equal to $abcd/10{,}000$. In order for this fraction to reduce to $1/n$, n would have to divide the denominator, which is of the form 10^k and therefore only has prime factors equal to 2 or 5.

5.



Since $72 = 2 \times 2 \times 2 \times 3 \times 3$, the other graph with the same shape will be that of $108 = 3 \times 3 \times 3 \times 2 \times 2$, as shown below.



Lecture Two

1. The following answers are subsets: a, b, and e.

2. **a.** Each die has 6 possible outcomes, so there are $6^5 = 7776$ possibilities.

b. The answer is $2(5!) = 240$. To see this, we break the problem into 2 cases. Either the dice are 1, 2, 3, 4, 5 or they are 2, 3, 4, 5, 6. For the first case, there are 5 choices for the 1, then 4 choices for the 2, then 3 choices for the 3, then 2 choices for the 4, then 1 choice for the 5, and therefore 1, 2, 3, 4, 5 can appear 5! ways. Likewise, 2, 3, 4, 5, 6 can also appear 5! ways.

c. First, we decide which 3 dice will contain the triple, which can be done $\binom{5}{3} = 10$ ways; the remaining 2 dice will contain the double. Then there are 6 ways to choose the tripled value, followed by 5 ways to choose the doubled value. Altogether, there are $10 \times 6 \times 5 = 300$ full houses.

d. Answer: $6^4 \times 3 = 3888$. One way to see this is that the red, yellow, green, and blue dice can be chosen freely, but then the purple die will have only 3 possibilities that will ensure an even total. Specifically, if the first 4 dice sum to an even total, then the purple die must be even (3 choices), and if the first 4 dice sum to an odd total, then the purple die must be odd (again, 3 choices). (This problem would have been much trickier with 7-sided dice! For that, you would need to break the problem into 3 cases, depending on whether there were 4, 2, or 0 odd numbers among the dice.)

Lecture Three

1. **a.** (I, D, $\geq$1).

b. (D, D, unrestricted).

c. (D, D, unrestricted).

d. (D, D, $\leq$1).

e. (I, D, $\leq$1).

f. (D, D, $\leq$1).

g. (D, I, $\geq$1).

h. (D, I, unrestricted).

2. $S(10, 1) = 1$, and $S(10, 2) = 2^9 - 1$, since the allocation can be described by choosing any subset of $\{1, \ldots, 9\}$ (except for the entire set) to appear in the bag with candy 10. $S(10, 9) = \binom{10}{2}$, since there will be 2 candies in 1 bag, and everything else will be a singleton. $S(10, 10) = 1$. In general, $S(n, 1) = 1$, $S(n, 2) = 2^{n-1} - 1$, $S(n, n-1) = \binom{n}{2}$, and $S(n, n) = 1$.

3. There is only 1 way to express the number n as the sum of 1 number (namely, $n = n$), so $p_1(n) = 1$. Likewise, there is only 1 way to express the number n as the sum of n numbers (namely, $n = 1 + 1 + 1 + \cdots + 1$), so $p_n(n) = 1$. Also, $p_{n-1}(n) = 1$, since 1 bag will have 2 candies and the rest of the bags will have 1. Equivalently, there is only 1 way to write the number n as the sum of $n - 1$ numbers where order does not matter, namely, $n = 2 + 1 + 1 + \cdots + 1$. $p_2(10) = 5$, since the smaller of the 2 bags will have 1, 2, 3, 4, or 5 candies. In general, when n is even, $p_2(n) = n/2$, and when n is odd, $p_2(n) = (n - 1)/2$.

4. To allocate 6 identical candies into 4 identical bags, there are 2 possible situations: (a) 1 bag gets 3 candies and the other 3 bags each get 1, or (b) 2 bags get 2 candies and 2 bags get 1. The first situation can happen $\binom{6}{3} = 20$ ways. The second case can happen $3\binom{6}{4} = 45$ ways. Choose which 4 candies a, b, c, and d will be in the double bags; then they can be allocated 3 ways: $\{a, b\}\{c, d\}$, $\{a, c\}\{b, d\}$, or $\{a, d\}\{b, c\}$. Altogether, we have $S(6, 4) = 20 + 45 = 65$.

5. $p_4(6) = 2$, since there are 2 possibilities: Either 1 bag gets 3 candies and the others each get 1, or 2 bags get 2 candies and 2 bags get 1.

Lecture Four

1. By adding consecutive entries of row 7, the eighth row is 1, 8, 28, 56, 70, 56, 28, 8, 1. Starting on the left with $\binom{8}{0} = 1$, we get $\binom{8}{3} = 56$.

This can also be obtained by factorials: $\binom{8}{3} = \frac{8!}{3!5!} = \frac{8 \times 7 \times 6}{3 \times 2 \times 1} = 56$.

2. The result is obtained by the binomial theorem: $\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} = (x+y)^n$.

Our identity is obtained by setting $x = 2$ and $y = 1$.

3. A combinatorial proof means showing that the left and right sides of an equation are equivalent solutions to the same counting question. Here, our counting question is "If a deck of n cards is dropped, how many ways can an even number of cards be face up?"

Answer 1: We can break this into cases that consider whether 0 cards are face up or 2 cards or 4 cards or 6 cards and so on, which gives us $\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\binom{n}{6}+\cdots$ ways.

Answer 2: On the other hand, we can create an even subset, card by card. For cards 1 through $n - 1$, there are 2 free choices, but there is only 1 choice for the n^{th} card. Thus there are 2^{n-1} ways.

Since answers 1 and 2 are both correct, they must be equal, and the conclusion follows.

4. Here, the combinatorial question is "How many ways are there to choose 4 hockey players from 10 players (wearing jerseys numbered 1 through 10)?"

Answer 1: There are $\binom{10}{4}$ ways to choose 4 players from 10.

Answer 2: Consider the largest jersey number in the subset. How many of these subsets have player 10 on the team (that is, have largest jersey number 10)? There are $\binom{9}{3}$ ways to choose the other 3 players. How many have largest jersey number 9? These subsets contain player 9 (and not player 10) and contain 3 other players from jerseys numbered 1 through 8, which can be chosen $\binom{8}{3}$ ways. Continuing this logic, we see that for $4 \le m \le 10$, the number of size-4 subsets with largest jersey number equal to m is $\binom{m-1}{3}$. Hence altogether, there are $\binom{3}{3}+\binom{4}{3}+\binom{5}{3}+\binom{6}{3}+\binom{7}{3}+\binom{8}{3}+\binom{9}{3}$ subsets, as desired.

5. Imagine that we play 8 more games (allowing for the possibility that some player may end up with more than 10 points). Among the 2^8 equally likely scenarios, the first player wins the match by winning at least 4 of these 8 games. Looking at row 8 of Pascal's triangle, this happens with probability (70 + 56 + 28 + 8 + 1)/256 = 163/256. The first player loses by winning 3 games or fewer, with probability (1 + 8 + 28 + 56)/256 = 93/256. Hence the $100 should be split by giving $100(163/256) = $63.67 to the first player and $100(93/256) = $36.33 to the second player.

Lecture Five

1. This is the same as the question "How many size-100 multisubsets can exist of {1, 2, 3, 4}?" where w denotes the number of 1s, x denotes the number of 2s, and so on. For example, the multisubset {1, 1, 1, 1, … , 1, 3} represents the solutions $w = 99$, $x = 0$, $y = 1$, $z = 0$. Hence the answer is $\left(\!\!\binom{4}{100}\!\!\right) = \binom{103}{100} = \binom{103}{3} = \frac{(103)(102)(101)}{3!} = 176,851.$

2. Once we have decided to use at least one 1, 2, 3, and 4, the problem reduces to solving $w + x + y + z = 100 - 4 = 96$, so the answer is $\left(\!\!\binom{4}{96}\!\!\right) = \binom{99}{96} = \binom{99}{3} = \frac{(99)(98)(97)}{3!} = 156,849.$

3. **a.** This is just the number of size-5 subsets of {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} (since each subset can be arranged in increasing order in just 1 way), so the answer is $\binom{10}{5} = 252.$

b. These are just the size-5 multisubets of {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. For example, the zip code 03399 is represented by the multisubset {0, 3, 3, 9, 9}, so the answer is $\left(\!\!\binom{10}{5}\!\!\right) = \binom{14}{5} = 2002.$

4. The word "MISSPELLINGS" has 3 Ss, 2 Ls, 2 Is, and 1 apiece of M, P, E, N, and G. So the answer is the multinomial coefficient $\binom{12}{3,2,2,1,1,1,1,1} = \frac{12!}{3!2!2!1!1!1!1!1!} = 19,958,400.$

5. This is the number of ways to arrange the number 122333444, which is $\binom{9}{3,3,2,1} = \frac{9!}{3!3!2!1!} = 5040.$

Lecture Six

1. The number of multiples of 3 is 100/3, rounded down to 33; there are 100/4 = 25 multiples of 4; and there are 100/5 = 20 multiples of 5. The number of multiples of 3 and 4 is 100/12, rounded down to 8, and so on. Thus by the principle of inclusion-exclusion, the answer is 100 − 100/3 − 100/4 − 100/5 + 100/12 + 100/15 + 100/20 − 100/60 (where each fraction is rounded down) = 100 − 33 − 25 − 20 + 8 + 6 + 5 − 1 = 40.

2. With no restrictions, EXCLUSION can be arranged 9! ways. There are 7! ways that include SIX (since we can think of SIX as a block to be arranged with 6 other letters), 5! that include OUNCE (a block with 4 other letters), and 3! that contain SIX and OUNCE (and a single letter L). Hence the answer is 9! − 7! − 5! + 3! = 357,726.

3. Such a hand must have 2 cards of 1 suit and 1 card of each of the other suits. So the answer is $4\binom{13}{2}13^3 = 685,464,$ since there are 4 ways to choose the doubled suit, and the rest of the product gives the number of ways to assign values to each suit.

4. Clearly, $D_1 = 0$. $D_2 = 1$ (counts the derangement 21), $D_3 = 2$ (counts 231 and 312), and $D_4 = 9$ (counts 2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321). We verify the formula when $n = 4$: $D_4 = 4!(1 - 1/1! + 1/2! - 1/3! + 1/4!) = 24 - 24 + 12 - 4 + 1 = 9.$

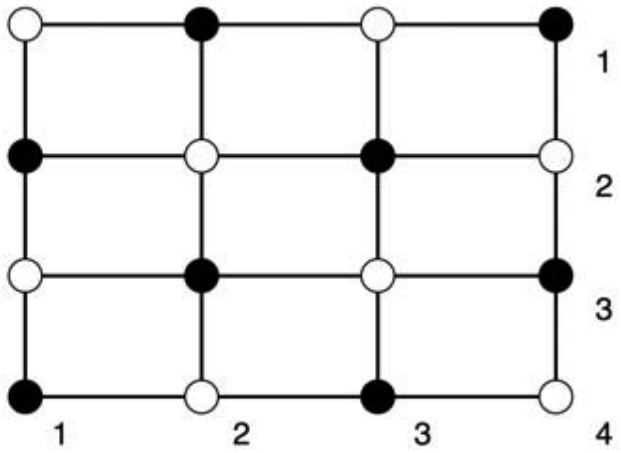
5. This is the same as asking how many ways 7 homework assignments can be returned so that exactly 3 students get their homework back. First decide which 3 numbers are in their natural positions, then arrange the remaining 4 numbers so that none of those numbers is in its natural position. This can be done $\binom{7}{3}D_4 = 35(9) = 315$ ways.

Lecture Seven

1. The pattern is

$1 + 2 + 3 + \cdots + (n - 2) + (n - 1) + n + (n - 1) + (n - 2) + \cdots + 3 + 2 + 1 = n^2$. The base case, when $n = 1$, says that $1 = 1^2$, which is clearly true. Next we state our induction hypothesis (IHOP), that the theorem is true for the number k. That is, $1 + 2 + 3 + \cdots + (k - 1) + k + (k - 1) + \cdots + 3 + 2 + 1 = k^2$. The goal is to show that it remains true for $k + 1$, that is, $1 + 2 + 3 + \cdots + (k - 1) + k + (k + 1) + k + (k - 1) + \cdots + 3 + 2 + 1 = (k + 1)^2$. This is the same sum as before, but it now includes a new $(k + 1)$ term and a new k term. Thus by IHOP, this new sum will be $k^2 + (k + 1) + k = k^2 + 2k + 1 = (k + 1)^2$, as desired.

2. Draw an $n \times n$ square with n^2 dots, and see how many dots appear on the diagonals. For example, the 4×4 square illustrates that $1 + 2 + 3 + 4 + 3 + 2 + 1 = 4^2$.



3. When $n = 1$, the left side and right side are 0. When $n = 2$, the left side is $1 \times 2 = 2$, and the right side is $(1)(2)(3)/3 = 2$, so the base case is satisfied. Now assume the theorem is true for the number k—that is, that $(1 \times 2) + (2 \times 3) + (3 \times 4) + \cdots + [(k - 1) \times k] = (k - 1)k(k + 1)/3$. Our goal is to show that it remains true for the number $k + 1$, so we wish to show that $(1 \times 2) + (2 \times 3) + (3 \times 4) + \cdots + [(k - 1) \times k] + k \times (k + 1) = k(k + 1)(k + 2)/3$.

Applying the induction hypothesis to the first k summands, then factoring out $k(k + 1)/3$, the left side is equal to $(k - 1)k(k + 1)/3 + k(k + 1) = [k(k + 1)/3][(k - 1) + 3] = k(k + 1)(k + 2)/3$, as desired.

4. **a.** When $n = 0$, the left side is equal to $f_0 = 1$, and the right side equals $f_2 - 1 = 2 - 1 = 1$, so the base case is verified. Inductively, if $f_0 + f_1 + \cdots + f_k = f_{k+2} - 1$, then $f_0 + f_1 + \cdots + f_k + f_{k+1} = (f_{k+2} - 1) + f_{k+1} = f_{k+1} + f_{k+2} - 1 = f_{k+3} - 1$, as desired.

b. Combinatorially, ask the question "How many ways can you tile a board of length $n + 2$ with at least 1 domino?" On the one hand, there are $f_{n+2} - 1$ such tilings, since we count all tilings of length $n + 2$, except for 1 tiling consisting of all squares. On the other hand, there are f_n of those that end with a domino, f_{n-1} of those that end with a square preceded by a domino, f_{n-2} of those that end with 2 squares preceded by a domino, and so on down to the 1 (f_0) tiling that ends with n squares preceded by a single domino.

Lecture Eight

1. Using the recurrence, $a_2 = a_1 + 12a_0 = 11 + 12 = 23$, and $a_3 = a_2 + 12a_1 = 23 + 12(11) = 155$. The recurrence $a_n = a_{n-1} + 12a_{n-2}$ generates the polynomial $x^2 - x - 12 = (x - 4)(x + 3)$, which has roots 4 and −3. Thus, $a_n = c_1(4)^n + c_2(-3)^n$. To determine c_1 and c_2, we use the initial conditions. When $n = 0$, $c_1 + c_2 = a_0 = 1$. When $n = 1$, $4c_1 - 3c_2 = a_1 = 11$. Solving 2 equations in 2 unknowns, we see that $c_1 = 2$ and $c_2 = -1$. Thus $a_n = 2(4)^n - (-3)^n$.

2. **a.** When $n = 0$, $a_0 = 0$, since we have no more chips to wager, so we cannot reach our goal of 5 chips. Similarly, $a_5 = 1$, since if we have 5 chips, then we have reached our goal. If the number of chips is n, where $0 < n < 5$, then 1/3 of the time, we win a chip, giving us $n + 1$ chips and giving us a_{n+1} chance of success, and 2/3 of the time we lose a chip, giving us $n - 1$ chips, giving us a_{n-1} chance of success. Taking a weighted average of these 2 outcomes, we conclude that $a_n = (1/3)a_{n+1} + (2/3)a_{n-1}$.

b. The polynomial can be rewritten as $a_{n+1} = 3a_n - 2a_{n-1}$, which generates the polynomial $x^2 - 3x + 2 = (x - 2)(x - 1)$. Therefore, $a_n = c_1 2^n + c_2 1^n = c_1 2^n + c_2$. To find c_1 and c_2, we plug in the known values of $n = 0$ and $n = 5$. When $n = 0$, $c_1 + c_2 = a_0 = 0$, which means that $c_2 = -c_1$. When $n = 5$, $32c_1 + c_2 = 1$, which means that $c_1 = 1/31$, and $c_2 = -1/31$. Thus $a_n = 2^n/31 - 1/31$. In particular, $a_3 = 8/31 - 1/31 = 7/31$.

3. This time, everything is the same, but the recurrence says that for $0 < n < 5$, $a_n = (1/2)a_{n+1} + (1/2)a_{n-1}$. We rewrite this as $a_{n+1} = 2a_n - a_{n-1}$. This generates the polynomial $x^2 - 2x + 1 = (x - 1)^2$, which has 1 as a double root. Thus $a_n = c_1 1^n + c_2 n 1^n = c_1 + c_2 n$. When $n = 0$, $c_1 = a_0 = 0$. When $n = 5$, $c_1 + 5c_2 = 1$. Therefore $c_1 = 0$ and $c_2 = 5$, so $a_n = n/5$, and in particular $a_3 = 3/5$. This says that when the game is fair, the probability of success is directly proportional to the number of chips that you have at the beginning.

4. **a.** How many flagpoles of height n can be created? Denote the answer by a_n. Then $a_0 = 1$ denotes the empty flagpole; $a_1 = 1$ counts the single red flag; $a_2 = 3$ counts RR, W, and B, which all have height 2; $a_3 = 5$ counts RRR, RW, RB, WR, and BR; and $a_4 = 11$ counts RRRR, RRW, RRB, RWR, RBR, WRR, WW, WB, BRR, BW, and BB.

b. For $n \geq 2$, the number of flagpoles of height n with a red flag on the bottom is a_{n-1}, the number that start with a white flag on the bottom is a_{n-2}, and the number that start with a blue flag on the bottom is a_{n-2}. Therefore $a_n = a_{n-1} + 2a_{n-2}$.

c. The recurrence generates the polynomial $x^2 - x - 2 = (x - 2)(x+ 1)$, which has roots 2 and -1. Therefore $a_n = c_1(2)^n + c_2(-1)^n$. Setting $n = 0$ and $n = 1$ gives us $c_1 + c_2 = a_0 = 1$ and $2c_1 - c_2 = a_1 = 1$. Solving this system of equations gives us $c_1 = 2/3$ and $c_2 = 1/3$. Therefore $a_n = (2/3)2^n + 1/3(-1)^n$.

5. The recurrence generates the polynomial $x^3 - 7x^2 + 14x - 8 = (x - 1)(x - 2)(x - 4)$. Therefore, $a_n = c_1(1^n) + c_2(2^n) + c_3(4^n)$. Applying the initial conditions, we get $c_1 + c_2 + c_3 = a_0 = 1$, $c_1 + 2c_2 + 4c_3 = a_1 = 1$, and $c_1 + 4c_2 + 16c_3 = a_2 = 7$, which has solution $c_1 = 3$, $c_2 = -3$, $c_3 = 1$. Therefore, $a_n = 3 - 3(2^n) + 4^n$.

6. Since $a_n = 3(2^n) - n2^n + 2(-3)^n$, we see that 2 is a double root and -3 is a single root of the polynomial, which must therefore be $(x - 2)^2(x + 3) = (x^2 - 4x + 4)(x + 3) = x^3 - x^2 - 8x + 12$. Hence, the recurrence is $a_n = a_{n-1} + 8a_{n-2} - 12a_{n-3}$, with initial conditions $a_0 = 3(2^0) - 0(2^0) + 2(-3)^0 = 5$, $a_1 = 3(2) - 1(2) + 2(-3) = -2$, and $a_2 = 3(4) - 2(4) + 2(9) = 22$.

Lecture Nine

1. Since $12x + 27y = 3(4x + 9y)$ is always a multiple of 3, it cannot create every integer.

2. Since $13(-2) + 27(1) = 1$, we can create any integer m by multiplying the equation by m. For instance, to create the number 9, we have $13(-18) + 27(9) = 9$.

3. Since $133 - 91 = 42$, $\gcd(133, 91) = \gcd(91, 42)$. And since $91 - 2(42) = 7$, $\gcd(91, 42) = \gcd(42, 7) = 7$. Therefore $\gcd(133, 91) = 7$.

4. Reversing the equations in the last answer, we see that $7 = 91 - 2(42) = 91 - 2(133 - 91) = 3(91) - 2(133)$. Therefore, $x = -2$ and $y = 3$ is one way to do it. (There are other ways, too.)

5. The Fibonacci numbers begin $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, $F_8 = 21$, $F_9 = 34$, and so on. The even numbers listed are F_0, F_3, F_6, and F_9, so it is natural to suspect that F_n is even if and only if n is a multiple of 3. This pattern can be proved true by observing that the Fibonacci sequence begins even, odd, odd, even, odd, odd, even, odd, odd, and that this will continue forever, since even + odd = odd, odd + odd = even, and so on. Notice that this pattern remains true even if we replace $F_0 = 0$ with any even number and $F_1 = 1$ with any odd number but continue with the recurrence $a_n = a_{n-1} + a_{n-2}$.

Lecture Ten

1. $57 = 32 + 16 + 8 + 1$ and has binary representation $(111001)_2$.

2. $2520 = 2^3 3^2 5^1 7^1$.

3. Each positive divisor must be of the form $2^a 3^b 5^c 7^d$, where $0 \le a \le 3$, $0 \le b \le 2$, $0 \le c \le 1$, and $0 \le d \le 1$, so the number of positive divisors is $4 \times 3 \times 2 \times 2 = 48$.

4. $2520 = 2^3 3^2 5^1 7^1$ and $825 = 3^1 5^2 11^1$, so $\gcd(2520, 825) = 2^0 3^1 5^1 7^0 11^0 = 15$, and $\text{lcm}(2520, 825) = 2^3 3^2 5^2 7^1 11^1 = 138{,}600$.

5. Notice that $a^2 + b^2 = (a + bi)(a - bi)$, so it can be factored. Thus $17 = 4^2 + 1^2 = (4 + i)(4 - i)$ is not a Gaussian prime and neither is $109 = 10^2 + 3^2 = (10 + 3i)(10 - 3i)$.

Lecture Eleven

1. You would need to pull out at least 11 socks to be assured of a matching pair.

2. By the pigeonhole principle, with 40 people, there must be a month with at least 4 of their birthdays, since if each month had at most 3 people, then there could be at most $12 \times 3 = 36$ people.

3. Imagine that the numbers 1 and 99 are in the same box, 2 and 98 are in the same box, 3 and 97 are in the same box, … , 49 and 51 are in the same box, and 50 is in a box by itself. Thus we have 50 boxes, and by choosing 51 numbers, there must be at least 1 box that was chosen twice. Such a box must contain 2 numbers that sum to 100. The statement is false when we choose 50 numbers, since the numbers could have been 1, 2, … , 50, where every pair of numbers has a sum below 100.

4. Pennies, nickels, and quarters have values of 1¢, 5¢, and 25¢, all of which are odd numbers. It is impossible for an odd number of coins (25 of them in this case) to sum to an even number (500 in this case).

Lecture Twelve

1. **a.** For months of the year, we work mod 12.

b. For the last 2 digits of a 5-digit number, we work mod 100.

2. Using mod-9 arithmetic, $31{,}415 \equiv 3 + 1 + 4 + 1 + 5 = 14 \equiv 1 + 4 = 5 \pmod 9$, and $12{,}358 \equiv 1 + 2 + 3 + 5 + 8 = 19 \equiv 1 + 9 = 10 \equiv 1 + 0 = 1 \pmod 9$. Thus $31{,}415 \times 12{,}358 \equiv 5 \times 1 = 5 \pmod 9$.

3. Using mod-11 arithmetic, $31{,}415 \equiv 3 - 1 + 4 - 1 + 5 = 10 \pmod{11}$, and $12{,}358 \equiv 1 - 2 + 3 - 5 + 8 = 5 \pmod{11}$, so $31{,}415 \times 12{,}358 \equiv 5 \times 10 = 50 \equiv 6 \pmod{11}$. You can see that $50 \equiv 6 \pmod{11}$ by noting that 50 divided by 11 has a remainder of 6, or that 11 divides $50 - 6$, or by the alternating sum rule: $50 \equiv -5 + 0 = -5 \equiv -5 + 11 = 6$.

4. $(10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \cdot (0, 3, 0, 7, 3, 3, 8, 4, 0, C) = 0 + 27 + 0 + 49 + 18 + 15 + 32 + 12 + 0 + C = 153 + C$. So $153 + C$ must be a multiple of 11. Therefore, C must be 1, since 154 is a multiple of 11.

5. The numbers below 14 that are relatively prime to 14 are 1, 3, 5, 9, 11, and 13. Since $1 \times 1 \equiv 1$ and $3 \times 5 \equiv 1$, $9 \times 11 \equiv 1$, and $13 \times 13 \equiv 1 \pmod{14}$, the inverses of 1, 3, 5, 9, 11, and 13 (mod 14) are 1, 5, 3, 11, 9, and 13, respectively.

Lecture Thirteen

1. Using the prime factorizations of the numbers 2 through 12 and looking at the largest exponent achieved by each prime, we see that the least common multiple of these numbers is $2^3 3^2 5^1 7^1 11^1 = 27{,}720$.

2. We are looking for the smallest positive integer N for which $N \equiv 3 \pmod{13}$ and $N \equiv 8 \pmod{17}$, which we can solve by the Chinese remainder theorem. Since 13 and 17 are relatively prime, there exist x and y such that $13x + 17y = 1$. Using the Euclidean algorithm, if needed, we find this equation is satisfied by $x = 4$ and $y = -3$. Thus, by the "max + may" formula, $N \equiv (13)(8)(4) + (17)(3)(-3) = 263 \equiv 42 \pmod{221}$. Hence the band has 42 musicians.

3. For this problem, we combine the solution of the last problem, $N \equiv 42 \pmod{221}$, with $N \equiv 1 \pmod{7}$. To find x and y such that $221x + 7y = 1$, we can solve (by trial and error or Euclid) and find that this equation is satisfied by $x = 2$ and $y = -63$. Therefore $N \equiv (221)(1)(2) + (7)(42)(-63) = 442 - 18{,}522 = -18{,}080 \pmod{1547}$. Adding the smallest multiple of 1547 to $-18{,}080$ to make it positive, we see that $N = -18{,}080 + 12(1547) = -18{,}080 + 18{,}564 = 484$. It is worth checking that indeed $484 \bmod 221 = 42$ and $484 \bmod 7 = 1$.

4. **a.** With 22 cards, an outshuffle will take the card in position x and move it to position $2x \bmod 21$ (when $0 \le x < 21$; the card in position stays in position 21). We can represent this permutation in terms of cycles: (0)(1 2 4 8 16 11)(3 6 12)(5 10 20 19 17 13)(7 14)(9 18 15)(21). So the number of shuffles needed to restore the deck is the least common multiple of $\{1, 6, 3, 6, 3, 2, 3, 1\} = 6$. A quicker solution is to notice that after 6 shuffles, a card in position x will be sent to position $2^6 x = 64x \equiv x \pmod{21}$, so every card will be back to its original position.

b. For a deck of size N to be restored after 4 outshuffles, it must be the case that $2^4 x = 16x \equiv 1x \pmod{N-1}$ for every value of x. In particular, when $x = 1$, we must have $16 \equiv 1 \pmod{N-1}$. The largest value of $N - 1$ that can do this is 15, and therefore the largest deck that has this property contains exactly 16 cards.

5. This can be solved by the lucky method or the seed planting method. With the lucky method, notice that $3^6 = 729$ is 1 bigger than $728 = 91 \times 8$. Therefore $3^6 \equiv 1 \pmod{91}$. So by the power rule, $3^{90} = (3^6)^{15} \equiv 1^{15} = 1 \pmod{91}$. Multiplying both sides by 3 gives us $3^{91} \equiv 3 \pmod{91}$.

To compute it by seed planting, express $91 = 64 + 16 + 8 + 2 + 1$ as $(101011)_2$. Then by successive squaring of 3, with seeds planted at steps 1, 3, 5, and 6, we get:

Step 1: 3

Step 2: $3^2 = 9$

Step 3: $9^2 \times 3 = 243 \equiv -30 \pmod{91}$

Step 4: $(-30)^2 = 900 \equiv -10 \pmod{91}$

Step 5: $(-10)^2 \times 3 = 300 \equiv 27 \pmod{91}$

Step 6: $(27)^2 \times 3 = 2187 \pmod{91} = 3$.

Lecture Fourteen

1. The proper divisors of $220 = 2^2 5^1 11$ are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110—which sum to 284. The proper divisors of $284 = 2^2 71$ are 1, 2, 4, 71, and 142—which sum to 220.

2. Since $2^n - 1$ is prime, we shall denote it by the number p. The divisors of $x = 2^{n-1}p$ can be split into those divisors that do not use p $(1, 2, 4, \ldots, 2^{n-1})$ and those that do use p $(1p, 2p, 4p, \ldots, 2^{n-1}p)$. The first group sums to $2^n - 1$, which equals p. The second group sums to p^2. Therefore the sum of all the divisors is $p^2 + p = p(p + 1) = 2^n p = 2(2^{n-1}p) = 2x$. Hence x must be a perfect number.

3. The original statement: Let p be an odd prime. If $p \equiv 1 \pmod{4}$, then p is the sum of 2 squares.

The contrapositive statement: Let p be an odd prime. If p is not the sum of 2 squares, then p is not congruent to 1 (mod 4).

The converse statement: Let p be an odd prime. If p is the sum of 2 squares, then $p \equiv 1 \pmod{4}$.

To prove the converse statement, suppose that p is an odd prime and p is the sum of 2 squares, say $p = a^2 + b^2$. When looking at the numbers mod 4, there are only 4 essentially different numbers: 0, 1, 2, and 3. Squaring these numbers gives us 0, 1, 4, and 9, which are congruent to 0, 1, 0, and 1 (mod 4). Thus if $p = a^2 + b^2$, then p can only equal 0, 1, or 2 (mod 4)—it cannot equal 3 (mod 4). Thus, since p is odd, it must be equal 1 (mod 4).

4. By Fermat's little theorem, since 101 is prime, $2^{101} \equiv 2 \pmod{101}$. Since 2 is relatively prime to 101, we can divide both sides by 2 to get $2^{100} \equiv 1 \pmod{101}$. Alternatively, we can use Euler's theorem. Since 2 is relatively prime to 101, and since 101 is prime, $\phi(101) = 100$, and therefore $2^{100} \equiv 1 \pmod{101}$. Using the power rule, if we raise both sides to the 7^{th} power, we get $2^{700} \equiv 1 \pmod{101}$. Therefore $2^{703} \equiv 2^{700}2^3 \equiv 8 \pmod{101}$.

5. Since $2520 = 2^3 3^2 5^1 7^1$, $\phi(2520) = 2520(1 - 1/2)(1 - 1/3)(1 - 1/5)(1 - 1/7) = 576$. And since 11 is relatively prime to 2520, we know that $11^{576} \equiv 1 \pmod{2520}$. So we multiply by 11, getting $11^{577} \equiv 11 \pmod{2520}$.

Lecture Fifteen

1. Suppose n is composite. Then $n = ab$, where a and b are both bigger than 1. Now suppose to the contrary that n did not contain a divisor (besides 1) that was at most $\sqrt{n}$. Then a and b are both greater than $\sqrt{n}$, and therefore $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction.

2. Since $493 = 17 \times 29$ (the product of 2 primes), then the only numbers M that are not relatively prime to 493 are those numbers that are multiples of 17 or multiples of 29. There are 29 multiples of 17 below 493 and there are 17 multiples of 29 below 493, and we have counted the number 0 twice. Therefore there are $29 + 17 - 1 = 45$ numbers (between 0 and 493) that are not relatively prime to 493. So the probability of the condition described in the question happening is 45/493.

3. The deciphering number d satisfies the equation $de - \phi(n)f = 1$. Here, $n = 493 = 17 \times 29$, $\phi(n) = 16 \times 28 = 448$, and $e = 303$. We are looking for numbers d and f that satisfy $303d - 448f = 1$. We can find d and f using the Euclidean algorithm: Notice that $448 = 303 + 145$, $303 = 145(2) + 13$, $145 = 13(11) + 2$, and $13 = 2(6) + 1$. Working backward through these equations, we get $1 = 13 - 2(6) = 13 - [145 - 13(11)]6 = 67(13) - 145(6) = 67[303 - 145(2)] - 145(6) = 303(67) - 145(140)$. Therefore, $d = 67$ will be the bank's deciphering number.

4. Here, $p = 71$ and $q = 79$, so $n = pq = 5609$, and $\phi(n) = (p - 1)(q - 1) = 70 \times 78 = 5460$. We are told that $e = 101$, so we must find d and f so that $101d - 5460f = 1$. Here is another way to find d and f: Let $a = 5460$ and $b = 101$. Subtracting 54 times the second equation from the first gives us $a - 54b = 6$. Now subtract 16 times the third equation from the second to get $-16a + 865b = 5$. Finally, subtract the fourth equation from the third to get $17a - 919b = 1$. Thus $17(5460) - 919(101) = 1$. That is, $101(-919) + 5460(17) = 1$. So $d = -919$ is a solution, or equivalently, $d \equiv -919 \equiv 4541 \pmod{5460}$. So $d = 4541$ will do the trick.

5. For the bank to decipher C^*, it should raise it to the e^* power (mod n^*), which it can do since it knows e^* and n^*. It then raises that to the d power (mod n), which it also knows how to do. The reason this works is that $(C^*)^{e^*} \equiv (C^{d^*})^{e^*} = C^{d^*e^*} \equiv C \pmod{n^*}$. Then $C^e \equiv (M^d)^e = M^{de} \equiv M \pmod{n}$.

Lecture Sixteen

1. **a.** $V = \{1, 2, 3, 4, 5\}$.

$E = \{\{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}$.

b. The shortest path from 1 to 3 is 1, 5, 3.

c. G is Eulerian. It is connected, and every vertex has even degree. An Eulerian tour is 1, 4, 5, 3, 2, 5, 1.

d. The graph has no Hamiltonian cycle, so it is not Hamiltonian.

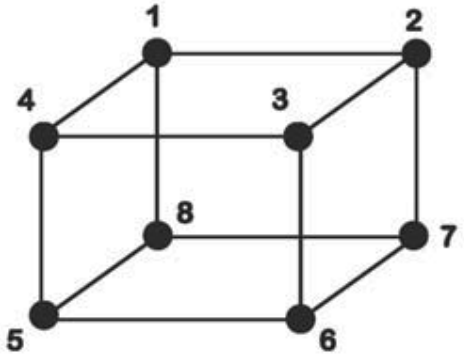
2. **a.** Since every pair of vertices is connected by an edge, there are $\binom{n}{2}$ edges.

b. K_n is connected, and every vertex has degree $n - 1$. Thus every vertex will have even degree if and only if n is odd.

3. Insert a new vertex z adjacent to x and y, creating a new graph, still connected, where every vertex (including x, y, and z) has even degree. Hence the new graph is Eulerian, and we can draw it as an Eulerian cycle that begins at z, takes first step to x, and therefore ends on the edge from y to z. In between the first and last step, we have drawn the original graph G as a trail.

4. The new graph will have exactly 2 vertices of odd degree, x and y, so it can be drawn as a trail that begins at x and ends at y.

5. **a.** The graph can be drawn like this.



b. It is not Eulerian because it has 8 vertices of odd degree.

c. It is Hamiltonian, since it has the Hamiltonian cycle 1, 2, 3, 4, 5, 6, 7, 8, 1.

Lecture Seventeen

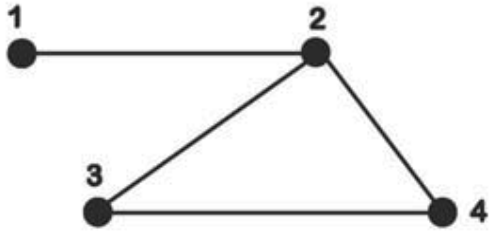
1. $A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$.

2. By matrix multiplication,

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 4 \end{pmatrix},$$

so the number of walks of length 4 from 1 to 5 is the (1, 5) entry of A^4, which is the dot product of (row 1 of A^2) and (column 5 of A^2): $(2\ 1\ 1\ 1\ 1) \cdot (1\ 1\ 1\ 1\ 4) = 2 + 1 + 1 + 1 + 4 = 9$.

3. One way to draw the graph would be this.



4. **a.** The transition probability matrix looks like this.

$$P = \begin{array}{c} \\ \text{S} \\ \text{C} \end{array} \begin{array}{c} \begin{array}{cc} \text{S} & \text{C} \end{array} \\ \begin{pmatrix} .5 & .5 \\ .25 & .75 \end{pmatrix} \end{array}$$

b. The (1, 2) entry of P^2 is the dot product of (.5, .5) and (.5, .75) = .25 + .375 = .625.

c. As P is raised to higher and higher powers, it will look like the matrix

$$P^* = \begin{array}{c} \\ \text{S} \\ \text{C} \end{array} \begin{array}{c} \begin{array}{cc} \text{S} & \text{C} \end{array} \\ \begin{pmatrix} p & 1-p \\ p & 1-p \end{pmatrix} \end{array},$$

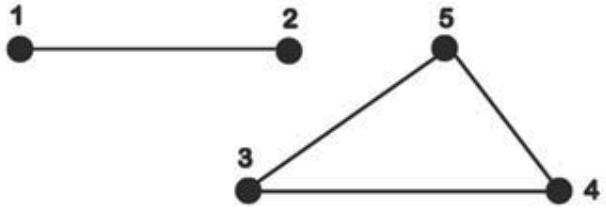
which should have the property that it should be unchanged when multiplied by P again. That is, $P^*P = P^*$, which means that

$$\begin{pmatrix} p & 1-p \\ p & 1-p \end{pmatrix}\begin{pmatrix} .5 & .5 \\ .25 & .75 \end{pmatrix} = \begin{pmatrix} p & 1-p \\ p & 1-p \end{pmatrix}.$$

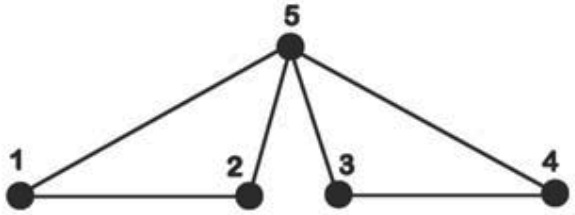
Equating the (1, 1) entry gives us $.5p + .25(1 - p) = p$, which has the solution $p = 1/3$. (Notice that we get the same solution if we equate any entry in the matrix.) Thus, in the long run, 1/3 of the days will be sunny.

Lecture Eighteen

1. **a.**



b.



c. Such a graph is impossible since vertex 5 must be adjacent to all 4 other vertices, including vertex 1. But then it would be impossible for $d(1) = 0$.

d. Such a graph is impossible since the sum of the degrees of the vertices is odd.

2. Equivalently, we prove that if the edges of K_{18} are colored red or blue, then it must contain an all-red K_4 or an all-blue K_4. Now consider vertex 18, which must contain at least 9 red edges or at least 9 blue edges, since otherwise it would have at most $8 + 8 = 16 < 17$ edges. Suppose that it has at least 9 red edges, going to vertices 1, 2, … , 9. Then among these 9 vertices, there must be an all-blue K_4 or an all-red K_3. If it has an all-blue K_4, then we are done. If it has an all-red K_3, using vertices a, b, and c, then along with vertex 18, we have an all-red K_4. The proof when vertex 18 has at least 9 blue edges is similar.

3. Each man can contribute $n!$ possible rankings, and each woman can contribute $n!$ possible rankings, so there are $(n!)^{2n}$ possible lists that the matchmaker can receive.

4. **a.** In round 1, men 1, 2, 3, 4, and 5 propose to women 3, 1, 5, 1, and 3, respectively. Woman 1 rejects man 2, and woman 3 rejects man 5. Men 2 and 5 then propose to women 3 and 4, respectively, but man 2 is rejected again. Man 2 now proposes to woman 5, who accepts him and rejects man 3. Man 3 proposes to woman 4, who rejects him. Then man 3 proposes to woman 3, who rejects him. Then man 3 proposes to woman 2, who accepts him. With no more unattached men or women, the algorithm terminates with stable pairings: man 1 with woman 3, man 2 with woman 5, man 3 with woman 2, man 4 with woman 1, and man 5 with woman 4.

b. Here, women 1, 2, 3, 4, and 5 propose to men 3, 3, 1, 5, and 5, respectively, with women 1 and 5 being rejected. Next women 1 and 5 propose to men 5 and 4, respectively, with woman 1 being rejected again. Then woman 1 proposes to man 1, who rejects her. Next woman 1 proposes to man 4, who accepts her and rejects woman 5. Woman 5 proposes to man 4, who accepts her and rejects woman 4. Woman 4 proposes to man 3, who accepts her and rejects woman 2. Woman 2 proposes to man 1, who rejects her. Then woman 2 proposes to man 2, who accepts her. The final stable pairing is man 1 with woman 3, man 2 with woman 2, man 3 with woman 4, man 4 with woman 1, and man 5 with woman 5.

5. **a.** There are 5 perfect matchings, since once we match vertex 6 to a vertex (5 possible choices), there is exactly 1 way to continue the perfect matching. For example, if we match vertex 6 with vertex 1, then we must match vertex 2 with 3 and vertex 4 with 5.

b. Applying the logic in part (a) above, if n is even, then W_n has exactly $n - 1$ perfect matchings, but if n is odd, then W_n has no perfect matchings.

Lecture Nineteen

1. **a.** Since every player loses at least 1 match, there is no emperor.

b. The only Hamiltonian path is 1, 2, 3, 5, 4.

c. Players 1, 2, and 3 are king chickens.

2. The complete graph K_n has $\binom{n}{2}$ edges, each of which has 2 possible orientations, so the number of tournaments on n vertices is $2^{\binom{n}{2}}$.

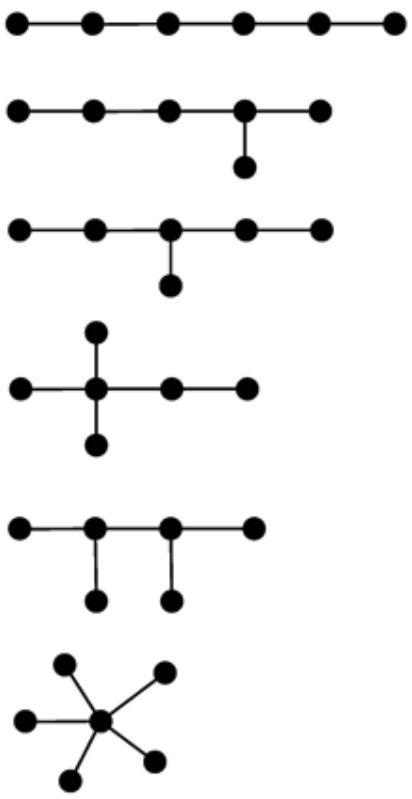
3. **a.** The shortest path from 3 to 2 is 3, 1, 2, so $d(3, 2) = 2$.

b. Suppose that $x \rightarrow y$, then $d(x, y) = 1$ and $d(y, x) > 1$. Otherwise, $d(y, x) = 1$ and $d(y, x) > 1$. Either way, we have $d(x, y) \neq d(y, x)$.

4. With 6 players, there are $\binom{6}{2} = 15$ matches played. It would be impossible for each player to have the same number of victories, since 6 does not divide into 15. In general, in a tournament with $2n$ players, the number of matches played is $\binom{2n}{2} = \frac{2n(2n-1)}{2} = n(2n-1)$, which is not divisible by $2n$, since the fraction $\frac{n(2n-1)}{2n} = \frac{2n-1}{2}$ is not an integer.

Lecture Twenty

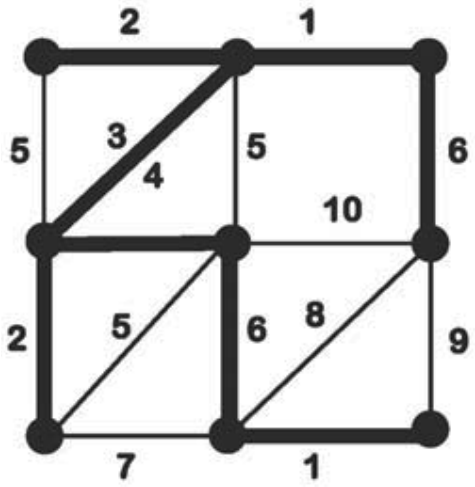
1.



2. The first tree can be labeled $6!/2 = 360$ ways. The second tree can be labeled $6 \times 5 \times 4 \times 3 = 360$ ways by labeling the vertex of degree 3, then its neighbor of degree 2, then the next vertex of degree 2, then the next vertex of degree 1. The third tree can be labeled $(6 \times 5 \times 4!)/2 = 360$ ways by labeling the vertex of degree 3, then its neighbor of degree 1, then the remaining 4 vertices from left to right (dividing by 2 since the same tree results when the labels are reversed). The fourth tree can be labeled $6 \times 5 \times 4 = 120$ ways by labeling the vertex of degree 4, then its neighbor of degree 2, then the next vertex of degree 1. The fifth tree can be labeled $\binom{6}{2}\binom{4}{2} = 90$ ways by deciding the labels for the vertices of degree 3, then for the vertex with the smaller label, choosing its 2 neighbors of degree 1. The sixth graph can be labeled 6 ways by choosing the label of the vertex of degree 5. Altogether, the number of labeled trees is $360 + 360 + 360 + 120 + 90 + 6 = 1296 = 6^4$.

3. Suppose that for every pair of vertices x and y, there exists a unique path from x to y. Then G is necessarily connected. Furthermore, G has no cycles, since if a cycle of length k exists, say, $v_1, v_2, \ldots, v_k, v_1$, then there would be more than 1 path from v_1 to v_k. Thus, since G is connected with no cycles, it must be a tree.

4. The minimum weight spanning tree, with total weight 25, is given below.



5. For the graph K_4, every vertex has degree 3, so

$D = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ and $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$. Therefore,

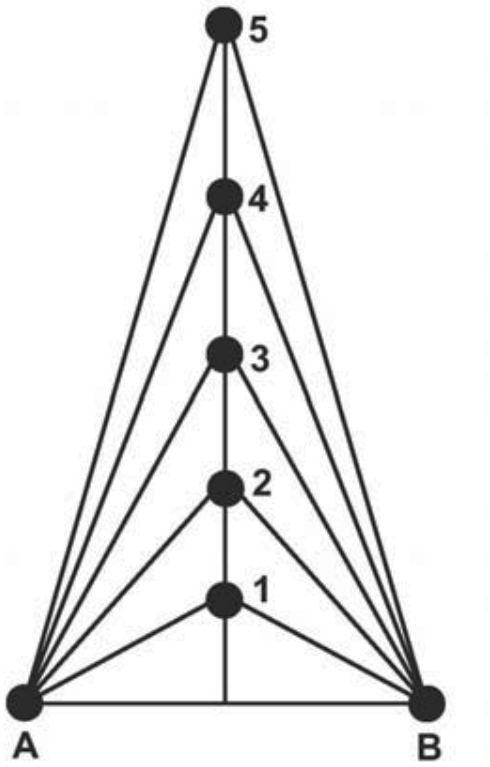
$D - A = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}$. Deleting the last row and column, the determinant of $\begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix}$ is $(27 - 1 - 1) - (3 + 3 + 3) = 16$.

The answer is not surprising, since this is the number of labeled trees on 4 vertices, which Cayley's formula tells us is equal to $4^2 = 16$.

Lecture Twenty-One

1. By Euler's planar graph theorem, $n - e + f = 2$, so $9 - 15 + f = 2$; therefore, the graph will have 8 faces.

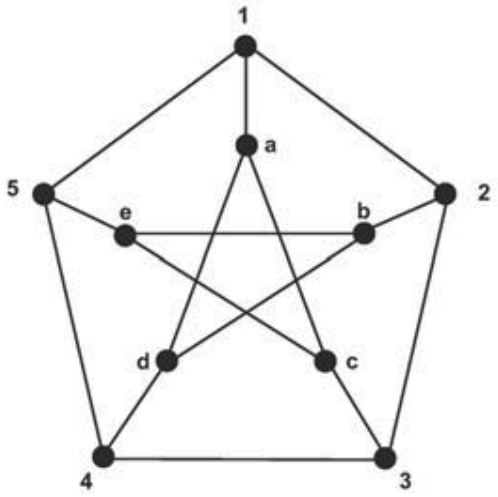
2. The graph can be redrawn as a plane graph as follows.



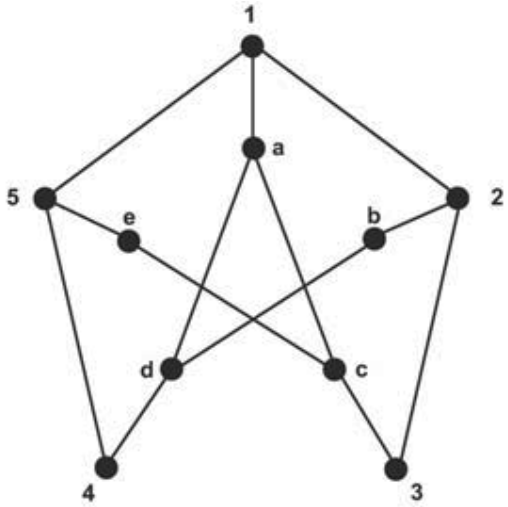
3. According to Euler's planar graph theorem, if the Petersen graph could be drawn as a plane graph, then the number of faces f would equal $2 - n + e = 2 - 10 + 15 = 7$. Thus its edge-face matrix would have 15 rows and 7 columns. Let X be the number of 1s in its edge-face matrix. Then counting row by row, since each edge borders at most 2 faces, we have $X \leq 2e = 30$. On the other hand, counting column by column, since each face (including the external face) uses at least 5 edges, then $X \geq 5f = 35$, which is a contradiction. Hence the Petersen graph is nonplanar.

4. First note that a subdivision of K_5 must contain at least 5 vertices of degree 4. Since the Petersen graph has no vertices of degree 4, it cannot contain a subdivision of K_5. We draw a subdivision of $K_{3,3}$ that is contained in the Petersen graph below. Notice that this graph does not have to use every edge of the Petersen graph.

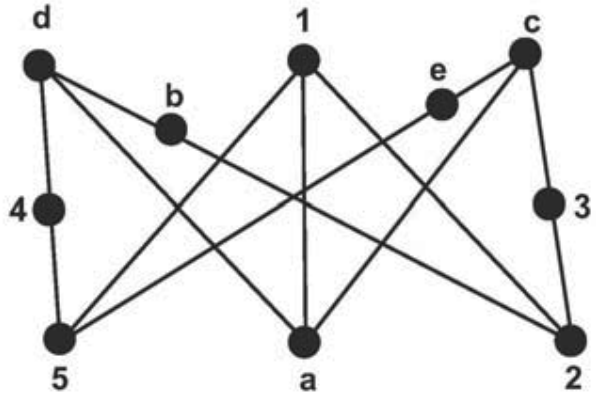
The Petersen graph



contains



which can be seen to be a subdivision of $K_{3,3}$ by redrawing it as



.

Lecture Twenty-Two

1. Since every pair of vertices is connected, any proper coloring of K_n must assign a different color to each vertex; therefore, the chromatic number of K_n is n.

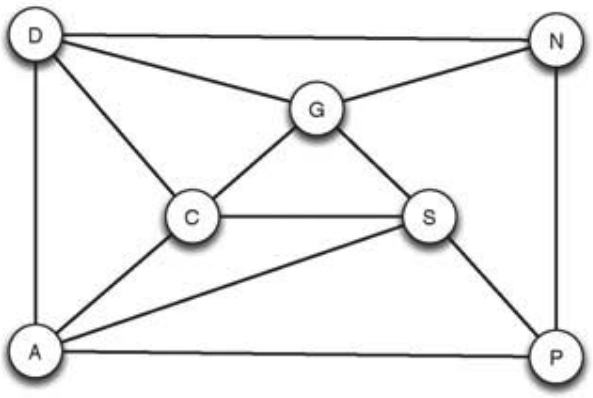
2. Proof by induction. Base case: When $n = 2$, a tree with 2 vertices has chromatic number 2. Inductively assume this is true for any tree with n vertices. Now consider a tree T with $n + 1$ vertices. Removing any leaf and its single edge, we obtain a tree T' with n vertices. By the induction hypothesis, T' has chromatic number 2 and can therefore be properly colored with exactly 2 colors. Returning the leaf to the tree, we can assign the leaf whichever color was not given to its neighbor. Therefore T can be properly colored with 2 colors (not with just 1 color), so it has chromatic number 2.

3. We prove that with m colors at your disposal, you can properly color a tree with n vertices in $m(m-1)^{n-1}$ ways. When $n = 1$, there are m ways to a color a tree with 1 vertex, and when $n = 2$, there are $m(m-1)$ ways to color a tree with 2 vertices (m choices for vertex 1 and then $m - 1$ choices for vertex 2). Inductively assume the theorem is true for trees with n vertices, and consider a tree T with $n + 1$ vertices. Removing a leaf from T results in a tree T' with n vertices, which by the induction hypothesis can be properly colored $m(m-1)^{n-1}$ ways. Returning the leaf to the tree, we can assign the leaf any of the remaining $m - 1$ colors. Therefore, T can be properly colored $m(m-1)^n$ ways.

4. Suppose, to the contrary, that a planar graph with n vertices had only 1 vertex of degree less than or equal to 5. Then the sum of the degrees of the vertices must be at least $6(n-1)$. Thus by the handshake theorem, the number of edges is at least $3(n-1) = 3n - 3$. But this is impossible, since a planar graph has at most $3n - 6$ edges.

5. This is an example of a planar graph where every vertex has degree 5. If every planar graph had to have at least 1 vertex of degree 4 or less, then this could have been used in an inductive proof of the 5-color theorem. (Remove the vertex of degree 4, then properly color the rest of the graph with 5 colors. Bring the degree-4 vertex back, and assign it a color that is different from its 4 neighbors.) A proof of the 4-color theorem could follow by using the Kempe chain argument that was used in the 4-color theorem.

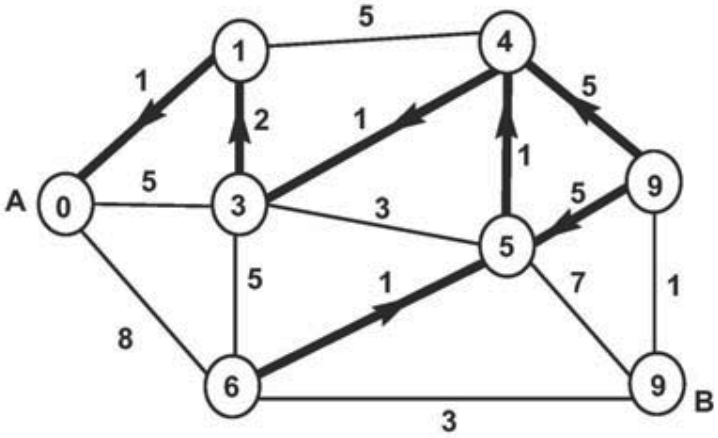
6. We create the graph below, where every vertex represents a course, and 2 vertices x and y are adjacent if a student wants to take course x and course y. The graph can be drawn as follows.



Each time slot is represented by a different color, and a legal assignment corresponds to a proper coloring of the graph, since 2 classes can be offered at the same time only if there is no student who wishes to take both classes. Since the graph is planar, it can be properly colored using 4 colors. (Find a way to do it.) To see that it cannot be done with 3 colors, we observe that vertices C, G, and S must get different colors (since they form a triangle), so we can color them 1, 2, and 3, respectively. But this forces A to get color 2, then D must get color 3, then N must get color 1, but now vertex P is adjacent to vertices with colors 1, 2, and 3, so it must receive a fourth color. Hence we can assign courses C and N in the first time slot, courses A and G in the second time slot, courses D and S in the third time slot, and course P in the fourth time slot.

Lecture Twenty-Three

1. A tree of shortest path is shown in bold below. The shortest path from A to B has length 9 and takes 6 steps.



2. Dijkstra's method can be used to determine whether the graph is connected. If a connected graph has n vertices and $n - 1$ edges, then it is necessarily a tree. (Why? Because otherwise, the graph would contain a tree with more than $n - 1$ edges, which is impossible.) Thus to determine whether the graph is a tree, simply count the edges. If it has $n - 1$ edges, then the graph is a tree and contains no cycles. If it has more than $n - 1$ edges, then the graph (connected) is not a tree and therefore contains cycles. Note that it is not possible for the graph to have fewer than $n - 1$ edges, since it is connected.

3. Problems a, b, c, and e are in the complexity class NP, since if we are given a solution to the problem, it can be verified efficiently. Problem d is not in NP, since it would require checking every subset to answer affirmatively, which cannot be done efficiently. Problem f is not in NP since it is not a decision problem.

Lecture Twenty-Four

1. We have established that a tiling of length $2n - 1$ that uses squares and dominoes must have at least n tiles. How many of these tilings use exactly k squares among their first n tiles? First we choose which k of the first n tiles are assigned to be dominoes. This can be done $\binom{n}{k}$ ways. Since the first n tiles contain k squares (of length 1) and $n - k$ dominoes (of length 2), these first n tiles will have a length of $k + 2(n - k) = 2n - k$. Since the length of the entire strip must be $2n - 1$, we still need to tile the rest of the strip, which has length $(2n - 1) - (2n - k) = k - 1$; this can be tiled in f_{k-1} ways. (Note that when $k = 0$, it is impossible for the first n tiles to be dominoes, since its length would be $2n$, which is too long. But this is accounted for since $f_{-1} = 0$.) Hence, for $0 \le k \le n$, the number of tilings of length $2n - 1$ with exactly k squares among its first n tiles is $\binom{n}{k} f_{k-1}$. Altogether, the total number of tilings of length $2n - 1$ is $\sum_{k=0}^{n} \binom{n}{k} f_{k-1}$, as desired.

2. You will always end up with the number 9. It is easy to see why if you look at your numbers mod 9. The first number will always have the same digit sum as the second number, so they are equivalent mod 9. In other words, $x \equiv y \pmod 9$, so $x - y \equiv 0 \pmod 9$; therefore, $x - y$ must be a multiple of 9 (but $x - y$ is not 0, since x and y are different numbers). Thus the digits of $x - y$ must sum to a multiple of 9.

3. The domino trick would not have worked with values 0 through 9, since its underlying graph would be K_{10}. The success of the domino trick with values 0 through 6 depended on the fact that its underlying graph, K_7, is Eulerian, since every vertex has even degree (6). But in the graph K_{10}, every vertex has odd degree (9), and K_{10} is not Eulerian. In fact, if we remove a single domino, then the resulting graph will have 8 vertices of odd degree (and 2 vertices of even degree), so it will not even be possible to create a chain of dominoes in the first place. But the trick would work if you secretly removed 4 dominoes with all different values—say, {0, 1}, {2, 3}, {4, 5}, and {6, 7}—since now there would be exactly 2 vertices of odd degree, vertices 8 and 9, which would have to be the endpoints of the chain.

4. You will end up on card 3 thanks to parity. When starting at card 1 (ace) or 5, you begin by taking an odd number of steps, which forces you to land on an even card, card 2 or card 4, so cards 1 (ace) and 5 can be safely removed. Next you take an odd number of steps, which forces you to land on the only odd-valued card, card 3.

Timeline

B.C.E.

300 ..... Euclid's *Elements* is written; 4 of the 13 books (books 7–10) address topics of number theory.

C.E.

1202 ..... Fibonacci numbers are first introduced by Leonardo of Pisa in his book *Liber Abaci*. They appear as an arithmetical exercise that involves the counting of pairs of rabbits.

1640 ..... Pierre de Fermat (1601–1655) discovers his "little" theorem, that for any prime p, p divides $a^p - a$. This was proved independently by Gottfried Leibniz in 1683 and Leonhard Euler in 1736.

1654 ..... The French mathematician Blaise Pascal discoveres Pascal's triangle when analyzing a problem that arose from gambling, called the problem of points. Pascal became the first mathematician to explore the triangle's many properties in his treatise, *Traité du Triangle Arithmétique*, published the following year.

1666 ..... The word "combinatorial" is first used in a modern sense by Gottfried Leibniz in his *Dissertatio de Arte Combinatoria* ("Dissertation Concerning the Combinational Arts").

1736 ..... Leonhard Euler (1707–1783) lays the foundations of graph theory by solving the bridges of Königsberg problem. That same year, he generalizes Fermat's little theorem using the phi function $\phi(m)$. (He discovered his planar graph formula, $n - e + f = 2$, around 1750.)

1801 ..... Carl Friedrich Gauss (1777–1855) publishes his book *Disquisitiones Arithmeticae*. This important book contains the first treatment of modular arithmetic.

1852 ..... The 4-color map problem is introduced to the mathematics community.

1876 ..... Édouard Lucas (1842–1891) proves that $2^{127} - 1$ is prime, which remained the largest known prime number until 1951.

1915 ..... Influential combinatorics textbook by Percy Alexander MacMahon appears, *Combinatory Analysis*.

1938 ..... Hardy and Wright publish their landmark *Introduction to the Theory of Numbers*.

1951 ..... J. C. P. Miller and D. J. Wheeler begin use of a computer to find much larger primes, including $(180)(2^{127} - 1)^2 + 1$.

1957 ..... *Introduction to Finite Mathematics* by John Kemeny, James Snell, and Gerald Thompson is the first mainstream textbook to survey discrete mathematics.

1958 ..... The first major textbook on graph theory appears, in French; translated into English in 1962.

1969 ..... The concept of the Erdös number is invented, named after prolific mathematician Paul Erdös.

1971 ..... The journal *Discrete Mathematics* begins publication.

1971 ..... Stephen Cook proves that the satisfiability problem is NP-complete.

1977 ..... The most famous method for public key cryptography, the RSA method, is discovered by 3 mathematically trained computer scientists, Ronald Rivest, Adi Shamier, and Leonard Adleman.

1977 ..... The 4-color theorem is proved by Wolfgang Haken and Kenneth Appel.

1995 ..... Andrew Wiles proves Fermat's last theorem.

2002 ..... A polynomial time algorithm is discovered to determine if a number is prime.

2008 ..... The number $2^{43,112,609} - 1$ becomes the largest prime number yet discovered.

Glossary

adjacency matrix: A matrix with (i, j) entry equal to the number of edges that connect vertex i to vertex j in a given graph.

algorithm: A method for solving a problem in a finite number of steps.

arrangement: A listing of objects where order matters, but repetition is not allowed.

Bézout's theorem (a.k.a. Bézout's identity): The greatest common divisor of a and b is the smallest positive number of the form $ax + by$, where x and y are integers. Named in honor of a more general result by Étienne Bézout (1730–1783).

Binet's formula: A closed form for the Fibonacci numbers. For $n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

binomial coefficient: $\binom{n}{k}$, pronounced "n choose k"; the number of size-k subsets of $\{1, 2, \ldots, n\}$, or equivalently, the number of ways to choose k objects from n, where order is not important and repetition is not allowed.

binomial theorem: It states that for any real or complex numbers x and y and any non-negative integer n,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

cancellation theorem: If $ax \equiv ay \pmod{m}$ and if $\gcd(a, m) = 1$, then $x \equiv y \pmod{m}$.

Carmichael number: A composite number that passes the Fermat primality test for every base. In 1994, 3 mathematicians proved that there must be an infinite number of Carmichael numbers. Named for American mathematician Robert Carmichael (1879–1967).

Cayley's formula: For $n \geq 1$, the number of trees with n vertices is n^{n-2}. Stated in 1854 without graph theory in a result by Arthur Cayley (1821–1895).

Chinese remainder theorem: If m_1 and m_2 are relatively prime, then there is a solution to the system of congruences $x \equiv a \pmod{m_1}$ and $x \equiv b \pmod{m_2}$. The solution is unique (mod $m_1 m_2$). Originated in China during the 3rd century C.E. but first published as a theorem by a Chinese government official in 1247.

chromatic number: The chromatic number of a graph G is the smallest number k for which G has a proper coloring that uses k different colors.

combinatorial proof: Showing that an equation is true by showing that the left side and right side of the equation are both solutions to the same counting question.

combinatorics: The mathematics of counting.

complete graph: A graph is complete if every pair of vertices is adjacent. The complete graph on n vertices is denoted by K_n.

complexity: The complexity of an algorithm is the number of steps to solve a problem of a given size. If a problem has size n, and the number of steps is bounded by a polynomial function of n, then the algorithm is considered to be efficient. If a decision problem has an efficient algorithm, then that problem belongs in the complexity class P.

composite: A positive number with 3 or more positive divisors.

congruence: We say $a \equiv b \pmod{m}$ ("a is congruent to b mod m") if m divides $a - b$; equivalently, a and b have the same remainder when divided by m.

contradiction, proof by: A proof technique that begins by assuming that the theorem is false, then showing how that leads to an impossible conclusion.

contrapositive: The contrapositive of the statement "If p, then q" is the statement "If not q, then not p." It is logically equivalent to the original statement.

converse: The converse of the statement "If p, then q" is the statement "If q, then p." It is not equivalent to the original statement.

cycle: A closed trail with no repeated vertices, except for the endpoints.

De Bruijn sequence: A sequence of binary code words where all 2^n binary code words of length n can be encapsulated in a single list of 2^n numbers. Named for Dutch mathematician Nicolaas Govert de Bruijn, whose work on such sequences appeared in 1946.

degree: The degree of a vertex v, denoted $d(v)$, is the number of vertices adjacent to v.

Dijkstra's algorithm: An efficient algorithm for finding the shortest path between any pair of vertices in a weighted graph. Introduced in 1959 by Dutch computer scientist Edsger Dijkstra (1930–2002).

division theorem: For positive integers a and d, there are unique integers q and r such that $a = dq + r$, where $0 \leq r < d$.

drawable: A graph G is drawable if it is connected and there exists a trail that uses every edge of G.

Euclid's algorithm: For any numbers a, b, x, $\gcd(a, b) = \gcd(b, a - bx)$. More specifically, $\gcd(a, b) = \gcd(b, a \bmod b)$.

Eulerian graph: A graph G is Eulerian if it is connected and there exists a closed trail that uses every edge of G.

Eulerian graph theorem: A graph is Eulerian if and only if it is connected and every vertex has an even degree.

Euler's planar graph theorem: For any connected planar graph with n vertices, e edges, and f faces, $n - e + f = 2$.

Euler's theorem (number theory): If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

factorial: $n!$ is the product $n(n - 1)(n - 2) \cdots (1)$. It counts the number of ways to arrange n distinct objects. For example, $4! = 4 \times 3 \times 2 \times 1 = 24$. The number 0! is defined to be 1.

Fermat primality test: If there exists an integer a such that a^n is not congruent to $a \pmod{n}$, then n is not prime.

Fermat's last theorem: For $n > 2$, there do not exist positive integers x, y, and z such that $x^n + y^n = z^n$.

Fermat's little theorem: For prime p and any integer a, $a^p \equiv a \pmod{p}$.

Fibonacci numbers: The numbers 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, … ; they are defined by $F_0 = 0$, $F_1 = 1$, and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. They were first introduced by Leonardo of Pisa in his book *Liber Abaci*.

forest: An unconnected graph with no cycles.

4-color theorem: A map of the counties of any state can always be colored in such a way that no adjacent counties are assigned the same color, and we need at most 4 colors to achieve this.

fundamental theorem of arithmetic: Also known as the unique factorization theorem; states that every positive number has a unique factorization into prime numbers.

Gaussian integer: A complex number of the form $a + bi$, where a and b are integers and i is an imaginary number whose square is -1.

Gaussian prime: A Gaussian integer that cannot be factored into Gaussian integers xy unless x or y is $1, -1, i$, or $-i$.

geometric proof: Proving a theorem by drawing a picture, often by decomposing a diagram in 2 different ways.

graph: A finite set of vertices, where some pairs $\binom{n}{n}$ of vertices are connected by an edge.

graph theory: The study of graphs—mathematical structures used to model pairwise relations between objects from a certain collection.

greatest common divisor: The largest positive integer that divides 2 numbers without remainder.

Hamiltonian graph: A graph that contains a cycle going through every vertex.

Hamiltonian path: A path that goes through every vertex of a given graph.

handshake theorem: The sum of the degrees of the vertices of a graph must be twice the number of edges.

important theorem: If d divides ab, and d is relatively prime to a, then d divides b.

induction: A proof technique for proving theorems by showing that if the theorem is true for the number k, then it will continue to be true for the number $k + 1$.

induction hypothesis (IHOP): The assumption in the inductive step (*see* **induction**) that the statement holds for some n.

inshuffle: A perfect shuffle where the top and bottom card do not stay at the top and bottom.

integer combination theorem: If $d|a$ and $d|b$, then $d|(ax + by)$ for any integers x and y.

king chicken theorem: In a tournament, x is a king chicken, or simply a king, if for every opponent y, either x beats y or there exists a player z such that x beat z and z beat y. In other words, a king is a player that can walk to any vertex in at most 2 steps.

Kuratowski's theorem: Every nonplanar graph contains inside it nonplanar graph K_5 or $K_{3,3}$ or a subdivision of K_5 or $K_{3,3}$ Proved by Polish mathematician Kazimierz Kuratowski in 1930. The capital K for the graphs K_n and $K_{m,n}$ is used in his honor.

least common multiple: The smallest positive number that is a multiple of 2 numbers.

Lucas numbers: An integer sequence named after the mathematician François Édouard Anatole Lucas. Like the Fibonacci numbers, each Lucas number is defined to be the sum of its 2 immediate previous terms. However, the first 2 Lucas numbers are 2 and 1 instead of 0 and 1. The sequence of Lucas numbers begins 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, … .

Markov chain: A random walk on a graph, where the probability of moving from vertex i to vertex j is given by a fixed probability p_{ij}.

matrix: A box of numbers.

minimum spanning tree: A tree that connects all the vertices of a weighted graph in such a way as to minimize the sum of the weights of the edges.

modulus: When doing modular arithmetic, you are interested in the remainders when dividing by a particular number m. The number m is called the modulus. The number x mod m is the remainder obtained when dividing x by m. In congruence statements, $x \equiv y \pmod{m}$ means that x and y have the same remainder when divided by m.

multichoose: The number $\left(\!\binom{n}{k}\!\right)$, pronounced "$n$ multichoose k," is the number of size-k multisubsets of $\{1, 2, \ldots, n\}$, or equivalently, the number of ways to choose k objects from n, where order is not important, but repetition is allowed.

multigraph: A graph that allows some pairs of vertices to be connected by more than 1 edge.

multinomial coefficient: The number $n!/(a!b!c!)$, where $a + b + c = n$, counts the ways to allocate n distinct pieces of candy so that child 1 gets a pieces, child 2 gets b pieces, and child 3 gets c pieces.

multiplicative inverse: Among the real numbers, the multiplicative inverse of the number b is the number $1/b$, since when we multiply them together we get the number 1. In modular arithmetic, when working with modulus m, the multiplicative inverse is a number c for which $bc \equiv 1 \pmod{m}$. With modulus m, b has a multiplicative inverse if and only if b is relatively prime to m.

multiset: A collection of objects where order does not matter, but repetition is allowed.

multisubset: The multiset X is a multisubset of the set Y if every element of X belongs to Y.

NP (nondeterministic polynomial): The set of decision problems where a yes answer can be verified in polynomial time.

number theory: The study of the natural numbers 0, 1, 2, 3, … .

outshuffle: A perfect shuffle where the top card stays on top and the bottom card stays on the bottom.

parity principle: A way of figuring out many mathematical conundrums by simply keeping track of odd numbers and even numbers.

partition number: $p_k(n)$ is the number of ways that the number n can be expressed as the sum of k positive integers, where order is not important. For example, $p_3(5) = 2$, since $5 = 3 + 1 + 1$ and $5 = 2 + 2 + 1$. The number $p(n)$ is the number of ways that n can be expressed as the sum of (any number of) positive integers, where order is not important. For example, $p(4) = 4$, since $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$.

Pascal's triangle: A triangle where, for $n \geq 0$, the elements of row n are the binomial coefficients $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}$.

path: A walk with no repeated vertices.

perfect shuffle: A shuffle where the deck is cut exactly in half, and the cards from each half are interlaced together perfectly. There are 2 types of perfect shuffles, inshuffles and outshuffles.

permutation: An arrangement of distinct objects; sometimes defined as the number of ways that k objects can be chosen from n objects, where order is important and repetition is allowed, and counted by the formula $n!/(n-k)!$. When $k = n$, the number of permutations is $n!$, pronounced "n factorial."

pigeonhole principle: If $n + 1$ objects are placed into n containers, then there must exist a container with at least 2 objects.

planar graph: A graph that can be drawn on a sheet of paper in such a way that none of its edges cross.

power theorem: If $a \equiv b \pmod{m}$, then $an \equiv bn \pmod{m}$ for any exponent $n \geq 0$.

prime: A positive number with exactly 2 divisors, 1 and itself.

prime important theorem: If prime p divides ab, then p divides a or p divides b. More generally, if prime p divides the product of n numbers, then p divides at least 1 of the numbers.

principle of inclusion-exclusion (PIE): A method for solving certain combinatorics problems that is as easy as PIE!

problem of points: A gambling problem, discovered by Blaise Pascal, which seeks to determine the appropriate settlement amount between 2 players, with a score of x to y, where the first person to reach n points wins d dollars.

proper coloring: The vertices of a graph G are properly colored if every vertex is assigned a color in such a way that no adjacent vertices have the same color. A similar definition applies to properly coloring the edges of a graph or the faces of a planar graph.

Ramsey number: The Ramsey number R(a, b) is the smallest value of n for which a coloring of the complete graph K_n using red and blue edges must result in an all-red K_a or an all-blue K_b. For example, R(3, 3) = 6.

Ramsey's theorem: For any positive numbers a and b, there is a number n such that if all edges of the complete graph K_n are colored red or blue, then there must exist an all-red K_a or an all-blue K_b.

relatively prime: Two numbers are relatively prime if their greatest common divisor is 1.

RSA method: An easily implemented method for public key cryptography. Published in 1977 by MIT computer scientists Ronald Rivest, Adi Shamir, and Leonard Adleman.

rule of product: The idea that if we have a ways of doing something and b ways of doing another thing, then there are ab ways of performing both actions.

rule of sum: The idea that if we have a ways of doing something and b ways of doing another thing and we cannot do both at the same time, then there are $a + b$ ways to choose one of the actions.

sequence: A listing of objects, where order matters and repetition is allowed.

set: A collection of distinct objects, where order does not matter.

skip sum identity: $\displaystyle\sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0.$

stable marriage problem: Given a collection of n eligible men and women, find a pairing of them so that no extramarital affairs will take place.

Stirling number: $S(n, m)$ denotes the number of ways of partitioning a set of n distinct elements into m nonempty subsets. These are also called Stirling numbers of the second kind. Stirling numbers of the first kind, also sometimes denoted by $S(n, m)$, denote the number of permutations of n elements that have exactly m cycles, or equivalently, the number of ways n people can sit around m identical circular tables so that no tables are unoccupied. Introduced by James Stirling (1692–1770).

subset: The set X is a subset of the set Y if every element of X belongs to Y.

tournament: A complete graph where every edge has an orientation. An edge that points from i to j can be thought of as player i defeating player j in a tournament where everyone plays everyone else in 1 game.

trail: A walk with no repeated edges. If the first and last vertex are the same, then the trail is closed.

traveling salesman problem: Find a Hamiltonian cycle in a weighted graph whose total weight is minimized.

tree: A connected graph with no cycles.

tribonacci numbers: A member of an integer sequence defined similarly to the Fibonacci numbers, except that each term equals the sum of the previous 3 terms in the series. The first few terms are 1, 1, 2, 4, 7, 13, 24, 44, and 81.

walk: A sequence of adjacent vertices where repetition is allowed.

weighted graph: A graph whose edges are assigned weights. The weight could reflect the cost of using the edge.

Wilson's theorem: Stated by John Wilson and proven by Joseph-Louis Lagrange in 1771: n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Biographical Notes

Binet, Jacques (1786–1856): French mathematician who worked in number theory and matrix theory. The closed form expression for the Fibonacci numbers is named after him.

Erdös, Paul (1913–1996): Hungarian-born mathematician, second only to Euler in all-time output, who authored or coauthored approximately 1500 papers. Choosing to have no formal professional position, he traveled from institution to institution to work with colleagues in number theory, probability, set theory, combinatorics, and graph theory. The notion of the Erdös number gave humorous recognition to his wide-ranging influence across 20th-century mathematics.

Euler, Leonhard (1707–1783): Swiss mathematician and scientist who worked in St. Petersburg and Berlin and was probably the most productive and influential mathematician of all time, introducing many ideas and notations still in use. He laid the foundations of graph theory by solving the bridges of Königsberg problem in 1736. That same year, he generalized Fermat's little theorem using $\phi(m)$, which later came to be called the totient function. He discovered his planar graph formula, $n - e + f = 2$, around 1750. He was father to 13 children, and he produced nearly half of his enormous mathematical output after losing nearly all his sight in 1771.

Fermat, Pierre de (1601–1655): French lawyer in Toulouse who was a leading contributor to number theory and analytic geometry. He discovered what is now called his little theorem (that any prime number p divides $a^p - a$) in 1640. His so-called last theorem famously appeared as a note in the margin of his copy of Diophantus's *Arithmetica*.

Fibonacci (a.k.a. **Leonardo of Pisa**; c. 1170–c. 1240): Italian mathematician from Pisa whose book *Liber Abaci* (1202) introduced what in the 19th century came to be called Fibonacci numbers as part of an arithmetical exercise that involved the counting of pairs of rabbits. Thanks to extensive travel in his youth, he learned the Hindu-Arabic numeral system, which he introduced to Europe in several important books.

Gauss, Carl Friedrich (1777–1855): Preeminent German mathematician and astronomer who spent most of his career at Göttingen and whose contributions span geometry, number theory, and analysis. He established mathematical rigor as the standard of proof, and his important *Disquisitiones Arithmeticae* (1801) contained the first treatment of modular arithmetic. Gauss's biographer quoted him as having said, "Mathematics is the queen of the sciences, and number theory is the queen of mathematics," while Gauss himself is often known as the Prince of Mathematics.

Hamilton, William Rowan (1805–1865): Irish mathematician whose invention of the algebra of quaternions later played a role in the development of quantum mechanics. Late in his career, his study of closed paths going exactly once through each vertex of a dodecahedron formed the basis of what became known as Hamiltonian graphs—an idea that he also turned into a board game (the Icosian Game).

Hardy, G. H. (1887–1947): English mathematician whose preference for pure mathematics was evident as early as the first edition of his influential textbook, *A Course of Pure Mathematics* (1908). Hardy arranged for Srinivasa Ramanujan to study and collaborate at the University of Cambridge during 1914–1919. Despite Hardy's disdain for applied mathematics—he once said, "No discovery of mine has made, or is likely to make directly, or indirectly, for good or ill, the least difference to anyone in the world"—he independently discovered a cornerstone of population genetics, later known as the Hardy-Weinberg law (1908). His cowritten *Introduction to the Theory of Numbers* (1938) remains in print today and was the considered the standard reference on the subject for much of the 20^{th} century.

Lucas, Édouard (1842–1891): French mathematician who worked in various areas of number theory. He discovered many interesting properties of the Fibonacci numbers, which he named after Fibonacci, and he also investigated a related sequence that we now call Lucas numbers. In 1876, he proved that $2^{127} - 1$ is prime, using methods for prime number testing that are still used today.

Markov, Andrey (1856–1922): Russian mathematician who followed early work in number theory with important results in the probability of related events, in which events are both random yet also linked to one another in what are now known as Markov chains.

Pascal, Blaise (1623–1662): French mathematician who discovered what came to be known as Pascal's triangle in 1654 when analyzing a problem that arose from gambling, called the problem of points. Pascal became the first mathematician to explore the triangle's many properties in his treatise *Traité du Triangle Arithmétique* (1655).

Ramanujan, Srinivasa (1887–1920): Largely self-taught Indian mathematician who is considered one of the mathematical geniuses of the 20th century, best known for his contributions to number theory and analysis. His work on integer partitions continues to intrigue and inspire number theorists and combinatorialists today.

Ramsey, Frank P. (1903–1930): British mathematician, economist, and philosopher whose combinatorial theorem regarding the coloring of graphs (e.g., the number of friends and strangers in a given group) led to efforts to identify what are now called Ramsey numbers and to so-called Ramsey theory, which studies the emergence of order as numbers become extremely large.

Bibliography

Benjamin, Arthur T., and Ezra Brown, eds. *Biscuits of Number Theory*. Vol. 34 of *Dolciani Mathematical Expositions*. Washington, DC: Mathematical Association of America, 2009. A collection of 40 exceptionally well-written articles; suitable for anyone taking a first course in number theory.

Benjamin, Arthur T., and Jennifer J. Quinn. *Proofs That Really Count: The Art of Combinatorial Proof*. Vol. 27 of *Dolciani Mathematical Expositions*. Washington, DC: Mathematical Association of America, 2003. More than 200 identities, many using Fibonacci numbers, Lucas numbers, and binomial coefficients, are given elementary combinatorial proofs.

Bogart, Kenneth P. *Introductory Combinatorics*. 2nd ed. New York: Harcourt Brace Jovanovich, 1990. A well-written, comprehensive intermediate-level combinatorics textbook.

Chartrand, Gary. *Introductory Graph Theory*. New York: Dover Publications, 1977. An excellent (and inexpensive!) introduction to graph theory, filled with many applications.

Dudley, Underwood. *Elementary Number Theory*. 2nd ed. New York: Dover Publications, 1978. An excellent (and inexpensive!) introduction to number theory, written with clarity and wit.

Edwards, A. W. F. *Pascal's Arithmetical Triangle: The Story of a Mathematical Idea*. Baltimore, MD: Johns Hopkins University Press, 2002. An accurate account of the origins of Pascal's triangle and some of its earliest applications.

Garey, Michael R., and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York: W. H. Freeman, 1979. The standard reference on the theory of NP-completeness.

Graham, Ronald L., Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. 2nd ed. Reading, MA: Addison Wesley, 1994. This is an intermediate-level discrete mathematics book that is suitable for someone who has completed this course. It combines CONtinuous math with disCRETE math, while devoting considerable attention to the evaluation of sums that arise in many combinatorial problems. Most pages are sprinkled with graffiti submitted by the authors and their students, providing additional insights and humor.

Gross, Benedict, and Joe Harris. *The Magic of Numbers*. Upper Saddle River, NJ: Pearson Prentice Hall, 2004. One of the best introductions to rigorous mathematical thinking. This is not so much a textbook to be studied as a book to be read and enjoyed.

Hardy, G. H., and E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. Oxford: Oxford University Press, 1978. Originally published in 1938, this classic of number theory was actually updated 40 years later by the second author. Although not the most elementary introduction to the subject, since some of the material requires calculus, it was the standard reference on the subject for decades.

Hopkins, Brian, and Robin Wilson. "The Truth about Königsberg."

The College Mathematics Journal 35 (2004): 198–207. A well-written article about what Euler proved and did not prove about the bridges of Königsberg.

Lovász, L., J. Pelikán, and K. Vesztergombi. *Discrete Mathematics: Elementary and Beyond*. New York: Springer-Verlag, 2003. This is probably the book that comes closest to capturing this *Discrete Mathematics* course, and I sometimes use it as a required textbook for my discrete math course at Harvey Mudd College.

Maurer, Stephen B. "The King Chicken Theorems." *Mathematics Magazine* 53 (1980): 67–80. A flock of results about pecking orders, describing possible patterns of dominance. (This article is viewable online at the website of the Mathematical Association of America, www.maa.org.)

Morris, S. Brent. *Magic Tricks, Card Shuffling, and Dynamic Computer Memories*. Washington, DC: Mathematical Association of America, 1998. Everything you ever wanted to know about the mathematics of perfect shuffles—and some magic tricks that can be performed once you have mastered the skill.

Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. 5th ed. New York: John Wiley and Sons, 1991. An intermediate-level textbook on number theory.

Rosen, Kenneth H. *Discrete Mathematics and Its Applications*. 5th ed. New York: McGraw-Hill, 2003. Probably the bestselling textbook on discrete mathematics, adopted at many colleges and universities.

Scheinerman, Edward. *Mathematics: A Discrete Introduction*. 2nd ed. Belmont, CA: Thomson Brooks/Cole, 2006. A terrific introduction to abstract reasoning and mathematical proof writing by way of discrete mathematical topics.

Silverman, Joseph H. *A Friendly Introduction to Number Theory*. Upper Saddle River, NJ: Prentice Hall, 1997. Like the title says, an extremely accessible introduction to the theory of numbers.

Stanley, Richard P. *Enumerative Combinatorics*. Vol. 1. Cambridge: Cambridge University Press, 1997. A graduate-level course in combinatorics.

Tucker, Alan. *Applied Combinatorics*. 4th ed. New York: John Wiley and Sons, 2002. A very readable textbook on combinatorics and graph theory, loaded with fun and interesting problems.

West, Douglas B. *Introduction to Graph Theory*. 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2001. An intermediate-level textbook on graph theory.

Wilf, Herbert S. *Algorithms and Complexity*. 2nd ed. Natick, MA: AK Peters, 2002. An intermediate-level textbook on the analysis of algorithms and computational complexity.

Wilson, Robin. *Four Colors Suffice: How the Map Problem Was Solved*. Princeton, NJ: Princeton University Press, 2002. A very readable account of the history and solution of the 4-color theorem.

Young, Robert M. *Excursions in Calculus: An Interplay of the Continuous and the Discrete*. Vol. 13 of *Dolciani Mathematical Expositions*. Washington, DC: Mathematical Association of America, 1992. Despite its title, it is really a book on number theory for people who have studied discrete mathematics and some calculus. The exposition is first-rate.

Notes

Notes

Notes

Notes